

**Order Form for Standard Goods and/or Services with Specialist Computer Centres PLC**

**Call-Off Contract under the HealthTrust Europe LLP Framework Agreement for the provision of Enterprise Level ICT Solutions for IT Hardware Products, Software, Programs, Applications, Associated Products, Services and Support – 2015 (reference number: SF049648) dated 8th December 2015.**

***Lot 2 – IT Software; Enterprise Level Software, Programs, Applications, Development, Associated Products, Services and Support***

SCC Ref OPP-2589046

|  |  |
| --- | --- |
| **The Authority** | ***Highways England Limited*** |
| **The Supplier** | Specialist Computer Centres plc |
| **HealthTrust Europe Contract Reference** | **HTE-01527.2** (Software) |

The Supplier and the Authority hereby agree as follows:

1. The Authority wishes to enter into a Contract in respect of the Goods and/or Services pursuant to the framework agreement between Health Trust Europe LLP and Supplier dated 8th December 2015 (the “Framework Agreement”).
2. The Contract incorporates, and the Supplier agrees to abide by, the following documents:
   * + 1. The Specification of the Authority’s requirements as appended at Appendix 1 overleaf;
       2. the Contract Price, as appended at Appendix 2 overleaf; and
       3. the Call-Off Terms and Conditions set out at Appendix A to the Framework Agreement (including the front page and all Schedules thereto).
3. The Authority acknowledges and agrees to the HealthTrust Europe Key Provisions set out at Schedule 1 of the Call-Off Terms and Conditions, in particular Clause 7 of Schedule 1 as stated below for the avoidance of doubt:
   * + 1. In the event that the Authority terminates its agreement with HealthTrust Europe (made pursuant to the provisions of the UHCW Framework) for convenience or otherwise, and such termination takes effect before the end of the Initial Term (as defined in the UHCW Framework) or in the event that the Authority’s agreement with HealthTrust Europe (made pursuant to the provisions of the UHCW Framework) expires without being renewed on or after such Initial Term, HealthTrust Europe shall notify the Supplier of such termination or expiry in accordance

with the provisions of Clause 15 of Schedule 1 of the Framework Agreement (“**Beneficiary**

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

* + - 1. The Authority acknowledges and agrees that the Supplier is subject to an activity based income (ABI) management charge in relation to any Orders placed by the Authority under the Framework Agreement.
      2. The Authority and the Supplier agree that (in addition to the Authority’s right to enforce the Contract) HealthTrust Europe may enforce any term of the Contract.

1. The Commencement Date of the Contract shall be ***11th January 2019***
2. The Term of this Contract shall be ***3 (three)*** years from the Commencement Date and may be extended in accordance with Clause 15.2 of Schedule 2 provided that the duration of this Contract shall be no longer than ***7 (seven)*** years in total.

1. **Data Protection**

* 1. The Parties acknowledge that the Authority is the Data Controller (as defined by the Data Protection Legislation) and the Supplier is the Data Processor (as defined by the Data Protection Act 1998) in respect of any Personal Data Processed under this Contract.
  2. For purposes of this Contract Data Protection Legislation means:

i. the General Data Protection Regulation (Regulation (EU) 2016/679) GDPR, the Law Enforcement Directive (Directive (EU) 2016/680) and any applicable national implementing

Laws as amended from time to time; ii. the Data Protection Act 1998 or from the date it comes into force, the Data Protection Act

2018 (DPA) to the extent that it relates to processing of personal data and privacy; iii. all applicable Law about the processing of personal data and privacy.

* 1. The Parties agree to comply with the terms of the Data Protection Protocol detailed in Appendix

3.

* 1. Notwithstanding any other provision of this Contract in the event of a conflict between the terms and conditions of this Contract and the terms of the Data Protection Protocol, the provisions of the Data Protection Protocol shall take precedence.
  2. The existing Schedule 3 of the Call Off Terms and Conditions Information Governance Provisions is replaced in its entirety with the attached Schedule 3 Call Off Terms and Conditions Information and Data Provisions

1. Time is of the essence as to any delivery dates under this Contract and if the Supplier fails to meet any delivery date this shall be deemed to be a breach incapable of remedy for the purposes of Clause 15.4.1(i) of Schedule 2.

1. For the purposes of Clause 4.2 of Schedule 2, the Authority shall visually inspect the Goods within 60 hours of the date of delivery of the relevant Goods.

1. The payment profile for this Contract shall be **See Appendix 2**

1. The Authority may terminate this Contract forthwith by notice in writing to the Supplier at any time on three (3) months’written notice. Such notice shall not be served within ***three (3)*** years of the Commencement Date.

1. The provision of Services

(A) The Services shall be provided by the Supplier at the Premises and Locations listed below: As per Appendix 2

1. The Contract Managers at the commencement of this Contract are:
   * + - 1. for the Authority:
         2. for the Supplier:
2. Notices served under this Contract are to be delivered to:
   * + - 1. for the Authority:
         2. for the Supplier:

1. In this Contract, unless the context otherwise requires, all capitalised words and expressions shall have the meanings ascribed to them by the Framework Agreement and/or Call-Off Terms and Conditions.
2. The following Appendices are incorporated within this Contract:

|  |  |
| --- | --- |
| **Appendix 1** | Authority Specification |
| **Appendix 2** | Contract Price |
| **Appendix 3** | Data Protection Protocol |

**Signed by the authorised representative of THE AUTHORITY**

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | Signature: | .. |
| Position: |  | Date: | 10/01/2019 |

**AND**

**Signed by the authorised representative of THE SUPPLIER**

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | Signature: |  |
| Position: |  | Date: | 10/01/2019 |

**Appendix 1**

**Authority Specification**

**Service Description**

# 1. Summary

The EUC Citrix Supplier shall provide a managed Citrix support service on its existing environment. This environment is currently hosted on The Supplier’s Sentinel PSN OFFICIAL Certified Government Cloud platform.

It is probable that during the period of this Contract that the Citrix environment is migrated to a public Cloud-based Solution, the Services defined in this Appendix are agnostic of the environment, where possible, upon which the EUC Citrix Services reside. Any agreed changes to the services and/or environment will be amended through the formal contract Change Control process.

At a high level the Citrix support function will include, but is not limited to, the following elements;

1.1 Platform availability @ 99.9% SLA

1.2 Monthly patching related to the Citrix platform

1.3 3rd Party Remote Access Support (1)

1.4 Service Operation Assistance

1.5 Service Design Input

1.6 Service Strategy Input

1.7 Continued Service Improvement

1.8 Netscaler Management (2)

1.9 Investigation Support

1.10 Monitoring capability (3)

1.11 Use the Authority’s Instance of ServiceNow as the call logging tool (4)

1.12 Actively work with the Service Desk, Service Management Team and HE’s ServiceNow Knowledge Team.

# Notes

1. See Section 12
2. The EUC Citrix Supplier will propose to move the NetScaler’s, including the Exchange pair, to a different platform, possibly F5 devices. This will be raised as an Operational Change Request, once this service is operational.
3. The EUC Citrix Supplier will raise an Operational Change Request to provide SCOM monitoring for the Citrix environment. There is currently no specific Citrix monitoring on the platform.
4. There is currently no integration between the Supplier and the Authority’s ServiceNow instances. The Supplier manually type in call related information to the Authority Service Now instance.
5. The Supplier Service Description is embedded below for information only.



SCC-HE Citrix Management Service

# Critical Dependencies

The Authority needs to ensure that an issue with two certificates, which require renewal at dates in January 2019 is resolved as soon as possible. This could impact the EUC Citrix partner’s ability to support and deliver the Citrix environment. This is a tier 1 risk to the early success of this contract and needs to be resolved by the Authority. The EUC Citrix Supplier must be absolved of all platform delivery responsibilities until this is resolved.

See Section 38 for the full risk register provided by the EUC Citrix Supplier as part of their Discovery Phase, plus the details of the first tranche of priority risks, requiring resolution within the first two months of the service ‘go live.’

# Definitions

**Citrix Service:** Shall mean the Service provided by the EUC Citrix Supplier, aligned to the content of this contract and within the Service Description embedded above.

**Citrix Environment:** Shall mean the Citrix Application and services provided by this application and 3 pairs of Netscaler load balancers.

The commencement of Service shall be on 11th January 2019 from the current incumbent Supplier, CGI, with knowledge transfer and shadowing activities happening before the commencement date and following a go-live decision from The Authority.

There will be an initial SLA holiday for the month of January 2019. During this time The Supplier will familiarise themselves with the Citrix Environment and carry out the tranche 1 risks, documented within section 38. At the end of the first month assuming that these risks have been resolved, then the EUC Citrix Supplier will perform against the agreed availability SLA for the remainder of the Contract term. If the EUC Citrix Supplier does not believe that the tranche 1 risks have been fully resolved, then an agreement will be reached with the Authority regarding extending the SLA holiday into the month of February 2019.

The following detailed requirements shall be delivered by the Supplier in delivering the EUC Citrix Service for the Authority.

1. The Authority currently provides a Citrix environment (running on Windows 2012 R2) accessed by both internal users and external partners. Internal users will access the Citrix Service via the Citrix Receiver application (which is currently not a supported version) on End User Devices (supported by the EUC Wintel Supplier) and thin-client devices (utilised in the Authority Outstations).

External partners will access the Citrix Service via a Remote Access Service (RAS) from external devices over the internet.

1. The EUC Citrix Supplier shall provide a fully managed Citrix Service, using the provided Citrix environment. The EUC Citrix Supplier shall support and maintain and manage the Service in accordance with Service Levels and Service Management requirements as specified in this document.

# 4. Support Services

4.1 The EUC Citrix Supplier shall provide remote 2nd and 3rd line support to all User Groups in accordance with their support needs across the Authority’s’ office locations.

4.2 The EUC Citrix Supplier shall provide the stated service:

4.2.1 Twenty-four (24) hours seven (7) days a week including bank holidays for Citrix Availability. Support for all Users provided by on call resources out of core hours;

4.3 The EUC Citrix Supplier shall comply with the Authority’s office security requirements and physical access arrangements and the HMG Security Policy Framework.

4.4 The EUC Citrix Supplier shall provide advice and guidance on the operability and inter-operability of Hardware and Software, where relevant to the EUC Citrix services.

4.5 The EUC Citrix Supplier shall advise the Authority of any developments in best practice, research findings, and User guidance in respect of its

obligations under this Agreement and in relation to the Management of Health and Safety at Work (Amendment) Regulations 2006 for IT.

4.6 The EUC Citrix Supplier shall co-operate with any third party employed by the Authority to carry out electrical testing of portable IT equipment which shall include any equipment provided or supported by the EUC Citrix Supplier.

4.7 The EUC Citrix Supplier shall implement all changes to the environment with minimum disruption to users, as agreed between the Authority and the Supplier.

# 5. Device Repair and Maintenance

5.1 The EUC Citrix Supplier shall schedule preventive maintenance to EUC Assets, within scope of this Citrix support contract, outside of normal business hours (07:00-19:00) and only within agreed maintenance windows, except in exceptional circumstances and with the agreement of the Authority.

5.2 The EUC Citrix Supplier shall comply with the Authority’s or 3rd Party Code of Connections should it wish to make connection to the Authority’s network for any reason.

# 6. Software Build Management

6.1 The EUC Citrix Supplier shall provide a Citrix build that is accessible from authorised accounts, both from the Authority’s end user estate and external suppliers with approved access.

6.2 The EUC Citrix Supplier shall ensure that any updates or changes to the Citrix environment does not result in Business Applications becoming unavailable and/or unusable, using the current knowledge base available and working in collaboration with the Application Maintenance partner.

6.3 In providing the Software Build Management Service, the EUC Citrix Supplier shall:

6.3.1 maintain and version control the Citrix Build by:

6.3.2 providing update releases of each Build including updates such as Operating System service packs, device driver updates and other changes;

6.3.3 managing the upgrade of the Citrix Build;

6.3.4 managing Build version information

6.3.5 document the Citrix Build and making that documentation available to the Authority;

6.3.6 work with other IT Suppliers to ensure policy settings of the Citrix environment are managed in accordance with the Authority’s policies;

# 7. Software Distribution

7.1 The EUC Citrix provider will work with other IT Suppliers to ensure that packaged applications are published correctly in the Citrix environment. This would be managed through the Change Management process.

# 8. Testing and Validation

8.1 The EUC Citrix Supplier shall work with the EUC Wintel Supplier to ensure that Application Packages are tested and within reason the application will load in the Citrix environment and not cause the other core applications to fail.

The demarcation lines of responsibility will need to be agreed between the Suppliers, as the EUC Citrix Supplier will not be responsible for any application support, remediation and packaging.

8.2 The EUC Citrix Supplier shall ensure that the Citrix Build is tested and within reason the environment will load and not cause the other core applications to fail on End User Devices.

8.3 In providing the Testing Service, the EUC Citrix Supplier shall:

8.3.1 test patches, where possible and relevant, for the Citrix environment, prior to incorporating them on the Citrix Build in accordance with the Authority’s policies;

# 9. Vulnerability Management

9.1 The EUC Citrix Supplier shall ensure the Citrix Environment is appropriately patched to secure against identified or known vulnerabilities related to the supported Citrix Environment. This will include processes, testing, where possible and remediation specific to the Citrix Environment.

9.1.1 monitoring the availability of anti-virus software updates, anti-virus signature updates and security releases relevant to the Citrix Service. The application of anti-virus to the Citrix Environment, at a server level, will be implemented as a change. This is not currently in scope.

9.1.2 monitor and manage the installation of patches appropriate to the Citrix environment.

9.2 In providing the Patching Service, the EUC Citrix Supplier shall:

9.2.1 test patches, where possible and relevant, for the Citrix Environment, prior to incorporating them on the Citrix Build in accordance with the Authority’s policies;

9.3 If the systems inherited by the EUC Citrix Supplier from the current incumbent

Supplier are unable to deliver the required functionality, The EUC Citrix Supplier shall work with the Authority to scope and specify the required systems and provide an appropriate impact assessment for the design and implementation of the system to deliver the required functionality.

9.4 The EUC Citrix Supplier shall implement security patches in line with the Release and Deployment Processes and Procedures, appropriate to the supported Citrix platform.

9.5 The EUC Citrix Supplier shall ensure Security updates and antivirus updates are maintained at latest levels, for critical updates within ten (10) working days, and for non-critical updates within one month, in arrears post their release from the vendor, so that security vulnerabilities are minimised. At the time of Contract signature, the Citrix Environment is not on the latest version therefore critical updates would not be typically available from Citrix. Once migration to the target cloud environment and upgraded to the latest Citrix version these timescales shall be fully applied.

# 10. Application Performance Monitoring Service

10.1 The EUC Citrix Supplier shall collaborate with the Service Management Supplier and other IT Suppliers to support the base lining and subsequent performance monitoring of any new or changed Applications. However, the EUC Citrix supplier is not responsible for the monitoring of application performance, only that of the Citrix platform.

10.2 The EUC Citrix Supplier shall provide a Capacity and Availability reporting service as agreed with the Authority’s' Service Management team (or equivalent Supplier)

# 11. Print Services

11.1 The EUC Citrix Supplier shall support the Print Supplier to provide a Print Service to provide Users access to printing facilities provided by other IT Suppliers in accordance with Authority’s policies and 3rd party contracts. However, the EUC Citrix Supplier is not responsible for the Print Service provided to the end users.

# 12. 3rd Party Remote Access Support

The EUC Citrix Supplier will work with other EUC Suppliers to ensure that remote access to the Citrix Environment is fully operational.

# 13. Impact Assessments

13.1 The Authority uses a process referred to as an Impact Assessment. This provides the Authority the ability to send work packages through to suppliers to evaluate and offer costs for the delivery of works and timescales entailed.

13.2 The EUC Citrix Supplier shall complete and return the Impact Assessment within five working days as per the normal business hours (0700hrs – 1900hrs, Monday – Friday). Responses to Impact Assessments will be measured as an KPI.

13.3 The EUC Citrix Supplier shall provide associated costs for the resources required to implement works if beyond the availabilities of the personnel already assigned to the delivery of Service. Costs for the inclusion of Capital Expenditure required to procure tools/products, must be included.

# 14. ITIL Aligned Best Practice

14.1 The Supplier is expected to deliver the Service in alignment with ITIL best practice

# 15. Demand Management

15.1 The EUC Citrix Supplier shall support the Authority and its Service Management Supplier in the management of demand for the Citrix Service. This will include controlling the environment capacity, related to the demand information, supplied by the Authority or their Partners, including:

15.1.1 making recommendations to reduce demands on the Citrix Service;

15.1.2 making recommendations on how Capacity Plans are/shall be affected by demand projections including the steps needed to meet demand projections;

15.1.3 support the Authority and Service Management Supplier in making available to the Authority's business units the mechanisms in place to control demand for the Citrix Service; and

15.1.4 making recommendations to the Authority and Service Management Supplier for improvements of the mechanisms to control and meet current and forecast demand for the Citrix Service.

15.1.5 The EUC Citrix Supplier shall review supplied demand information for the Citrix Service and will engage in reviews with the appropriate partners to ensure that demand requirements can be accommodated within the Citrix Environment.

# 16. Financial Management

16.1 The EUC Citrix Supplier shall provide EUC Service financial data to the Authority in accordance with the Financial Management Policies, Processes and Procedures.

16.2 The EUC Citrix Supplier shall provide EUC Service consumption data to the Service Management Supplier in accordance with the Service Operations Manual.

16.3 The EUC Citrix Supplier shall support the Service Management Supplier in resolving any discrepancies in EUC Service consumption data.

# 17. Service Portfolio Management

17.1 Where new business requirements identify the need for additional EUC Citrix Services, these shall be impact assessed to determine the effort to deliver the new business requirement through the EUC Citrix Service.

# 18. Service Risk Management

18.1 The EUC Citrix Supplier shall identify and mitigate any emergent risk to the provision of EUC Citrix Service.

18.2 The EUC Citrix Supplier shall advise the Service Management Supplier of any emerging risks, related to the management of the Citrix platform and shall provide a proposal of how such emerging risks should be addressed in accordance with the current ITSCM (IT Service Continuity Management) Plan,

where this exists and the Information Security Management Plan and ITSCM Policies and Procedures.

18.3 The EUC Citrix Supplier shall implement any measure identified to address any emerging risk which has been approved by the Authority under the direction of the Service Management Supplier. Such measures shall be implemented in accordance with the Service Request Process.

# 19. Availability Management

19.1 The EUC Citrix Supplier shall participate in regular availability risk reviews under the direction of the Service Management Supplier.

19.2 The EUC Citrix Supplier shall support the Service Management Supplier to schedule and coordinate any Planned Outages in accordance with the Availability Management Policies, Processes and Procedures to minimise disruption to Patterns of Business Activity. The reporting of this is to be jointly reviewed and agreed.

19.3 The EUC Citrix Supplier shall collect, analyse and maintain availability data and report on that data for EUC Services. Availability management reporting shall include availability, reliability, and maintainability. The reporting of this is to be jointly reviewed and agreed.

19.4 The EUC Citrix Supplier shall identify and rectify problem areas which impact or have the potential to impact availability.

19.5 The EUC Citrix Supplier shall assess the impact of planned changes against availability plans.

19.6 The EUC Citrix Supplier shall identify tactical and strategic risks to availability in the medium- to long-term and prepare mitigation plans.

19.7 The EUC Citrix Supplier shall, working with the Service Management Supplier, ensure the delivery of EUC Citrix Services meet agreed availability, design criteria and Service Levels

# 20. Capacity Management

20.1 The EUC Citrix Supplier shall produce and maintain Capacity Plans for the EUC Services that cater for:

20.1.1 fluctuations in business as usual capacity demand;

20.1.2 planned business change;

20.1.3 patterns of Business Activity;

20.1.4 revised or new Service Levels, as agreed between involved parties;

20.1.5 revised or new EUC Services, related to the Citrix platform;

20.1.6 ITSCM;

20.1.7 transition requirements; the impact of emerging technologies within the Service pipelinethrough the Operational Change Process.

20.2 The EUC Citrix Supplier shall advise the Service Management Supplier of predicted capacity shortfalls and propose solutions, impact, risks and cost, providing supporting evidence on a timely basis as needed.

20.3 The EUC Citrix Supplier shall take appropriate action or make recommendations to relieve capacity restrictions beyond agreed thresholds.

20.4 The EUC Citrix Supplier shall proactively report on resource capacity and resource utilisation.

20.5 The EUC Citrix Supplier shall recommend appropriate capacity thresholds in accordance with the Service Levels and the Capacity Management Policy, as Citrix Best Practise recommendations.

20.6 The EUC Citrix Supplier shall optimise resource utilisation in a cost-effective manner (Resource Capacity Management).

20.7 In the event that there are discrepancies between the EUC Service consumption information provided by the EUC Citrix Supplier, the EUC Citrix Supplier shall work with the Service Management Supplier to resolve such discrepancies

20.8 The EUC Citrix Supplier shall work with the Service Management Supplier to facilitate the optimisation of Capacity and increase or decrease Capacity for the EUC Citrix Service in order to maintain the operation of the Citrix Environment.

# 21. IT Service Continuity Management (ITSCM)

21.1 The EUC Citrix Supplier shall provide input into Authority’s IT Service Continuity Management plans in accordance with the Service Operations Manual.

21.2 The EUC Citrix Supplier shall provide a single point of contact for Business Continuity and Disaster Recovery planning, related communications and other activities within the scope of the EUC Services. This single point of contact shall be identified as a Key Person.

21.3 The EUC Citrix Supplier shall document and maintain priorities for backups,

Disaster Recovery and Business Continuity where applicable to the EUC

Citrix Services, based on the Authority’s business continuity requirements.

21.4 The EUC Citrix Supplier shall manage Service Continuity risks for EUC Citrix Services, including maintaining descriptions of possible and high probable crisis situations and incorporating mitigation and contingency actions into the ITSCM Plans (scenario planning).

21.5 The EUC Citrix Supplier shall collaborate with the Service Management Supplier to develop an agreed set of ITSCM Plans in accordance with the Service Operations Manual.

21.6 The EUC Citrix Supplier shall take part in ITSCM Awareness and Training for ITSCM related personnel as part of the ITSCM lifecycle. This ITSCM Awareness and Training will be provided by the Authority.

21.7 The EUC Citrix Supplier shall support the Service Management Supplier and the Authority in the production of Business Impact Analysis as and when required by the Authority.

21.8 The EUC Citrix Supplier shall comply with any improvements which need to be made to the ITSCM Plans. This engagement would be via the Change Management process.

21.9 The EUC Citrix Supplier shall ensure that the management and reporting of the EUC Citrix Services (omitting the Citrix Receiver) and Citrix components thereof are configured in a way that ensures the information captured can be used in planning IT Service Continuity for the IT services. This would be based on implementing the recommended tier 1 changes recorded within the risk register and this contract document.

# 22. Service Level Management

The EUC Citrix Supplier shall provide and deliver the EUC Services to the agreed availability and design criteria and proposed Service Levels, Service Level Targets and agreed Key Performance Indicators for new or changed EUC Services in a timely manner.

22.1 The EUC Citrix Supplier shall provide all relevant information relating to Service Levels, Service Level Targets and Key Performance Indicators for the EUC Citrix Service.

22.2 The EUC Citrix Supplier shall participate in negotiations to ensure all Service Levels for EUC Services are appropriate and in line with the IT Service Levels.

22.3 The EUC Citrix Supplier shall support the Service Management Supplier in the analysis of EUC Service performance to ensure completeness and appropriateness of content for presentation to the Authority.

22.4 The EUC Citrix Supplier will produce a monthly report for discussion as part of a monthly Governance review. The report will detail key elements of the service, SLA conformance and continual service improvements.

22.5 The EUC Citrix Supplier will seek to achieve the following SLAs:

22.5.1 Citrix Service Availability - 99.9% availability over a calendar month on a 24\*7 basis.

22.5.2 The service credits will be delivered as described below:

22.5.2.1 Up to a 1% rebate of the Monthly Charge for the failure of the Citrix Service to achieve the target availability by less than or equal to 1%.

22.5.2.2 This rebate will increase by up to an additional 1% for every additional 1% (or part there-of) failure to meet the target availability, up to a maximum of 10%. Examples of service credits are within the table below:

*Redacted*

22.5.2.3 The applicable Service Credit shall be deducted off the next invoice due to the Authority. This would be unless otherwise agreed with the Authority

22.5.2.4 Allowance by the EUC Citrix Supplier of Service Credits to the Authority shall be in full and final settlement of the EUC Citrix Supplier’s liability to the Authority for failure to meet the Service Levels during the reporting period.

22.5.2.5 Service Levels will only be calculated against the Citrix Environment availability and not against application availability. Service Credits against the loss of platform availability will not include other machines or applications impacted by that loss.

22.5.2.6 Service Credits will not be applied where it is determined that the EUC Citrix Supplier is not responsible for the cause of the breach in Citrix Service Availability performance.

22.5.2.7 Key Performance Indicators

|  |  |
| --- | --- |
| **Service Level** | **Key Performance Indicators** |
| 95% of Root cause identification tasks to be complete within 10  Problem working days (Monday-Friday) days of notification for Severity 1  management (KPI)  Incidents. | |
| Change management | 98% of changes successfully completed (subject to CAB approval). |
| Incident Resolution | 80% of P1 incidents resolved in 4 hours when the total of P1 incidents logged in the period is <10.  90% of P1 incidents resolved in 4 hours when the total of P1 incidents logged in the period is >10. |
| 80% of P2 incidents resolved in 8 hours when the total of P2 incidents logged in the period is <10.  90% of P2 incidents resolved in 8 hours when the total of P2 incidents logged in the period is >10. |
| Upgrade notification (KPI) | 98% of software upgrades are notified to the Authority Service Management team within 5 days of release. The software list is limited to Citrix Environment upgrades. |

22.6 If the Supplier does not achieve the availability SLA, or Key Performance Indicators then remediation steps will be defined and tracked to achieve ongoing conformance.

If the Supplier fails to achieve the Service Level Target in two (2) calendar months during a rolling six (6) month period, the Supplier will formally write to the Authority within twenty (20) working days from the end of calendar month of the second failure, detailing their action plan to avoid continued Service Level failures. The Authority upon receipt of the Supplier’s action plan will convene a meeting with Supplier’s Senior Management within ten (10) working days to discuss and confirm acceptance of the Supplier action plan. In the event that both parties cannot agree upon the action plan the matter will be escalated through the Governance process.

22.7

22.8 The Authority reserves the right to review and where applicable amend the

SLA’s with the EUC Citrix Supplier every 6 months from commencement of the contract, in agreement with the EUC Citrix supplier.

22.9 The EUC Citrix Supplier will seek to accurately respond to Impact Assessments within 5 working days.

# 23. Service Level Details and Measures

23.1 The objectives of these Service Level Agreements are to:

23.1.1 ensure that the Services are of a consistently high quality and meet the Service Levels and other requirements of The Authority;

23.1.1.1 provide a mechanism whereby the Service Levels, Key Performance Indicators (KPIs) and Service Credits can be modified over the Contract Period in response to the changing requirements of The Authority; and

23.1.1.2 incentivise the EUC Citrix Supplier to:

23.1.1.3 meet the Service Levels and KPIs;

23.1.1.4 promptly rectify any failure to meet the Service Levels or KPIs.

# 24. Service Level and KPI Principles

24.1.1 Any failure by the EUC Citrix Supplier to deliver the Services, and to achieve the Service Levels and KPIs will have an impact on The

Authority’s operational effectiveness and efficiency and subsequently its ability to fulfil its statutory obligations.

24.1.2 The Service Levels and KPIs are focussed on The Authority; reflect the needs of The Authority and represent the Services quality that is required by The Authority and its business units and end users.

24.1.3 The EUC Citrix Supplier shall work collaboratively with other The Authority IT Suppliers to deliver the ICT Services and ensure that the Service Levels and KPIs are met.

24.2 The objectives of the Service Credits and other related remedies are to:

24.2.1 ensure that the Services are of a consistently high quality and meet the Service Levels and other requirements of The Authority;

24.2.2 use Service Credits as a method of price adjustment to reflect poor performance in breach of the required Service Levels;

24.2.3 provide a mechanism whereby the Service Credit regime can evolve over the Contract Period as the profile of Services change; and

24.2.4 incentivise the Supplier to meet the Service Levels and work to remedy any failure to meet the Service Levels promptly. The EUC Citrix Supplier acknowledges that the Authority will, in all cases, prefer to receive the Services at the Service Level Target in preference to receiving the Service Credits. Consequently, the EUC Citrix Supplier shall, in all cases, seek to deliver the Services at or above the Service Level Target in preference to accepting a liability for Service Credits.

24.2.5 The Supplier shall be open, transparent and honest about the levels of performance and service quality the Supplier is achieving with The Authority and the Tower Service Suppliers.

# 25. Service Level Framework

25.1 The information in Paragraph 22.4 (above) sets out the Service Level Target that shall be measured and reported on by the Supplier, including the Service Level Target and associated Service Credits.

25.2 On a 6-monthly basis, The Authority and the EUC Citrix Supplier will meet to review the Service Levels and KPIs, and any associated Service Credits, and in addition on reasonable request from the Authority or the EUC Citrix Supplier in accordance with paragraph 25.4 above.

25.3 All KPIs that will be reported on by the Supplier alongside the Service Levels will be agreed between the EUC Citrix Supplier and The Authority, and reported on monthly.

25.4 In the event that:

25.4.1 any Services or component thereof, does not achieve the Service

Level Targets, KPIs or any other agreed performance measures, the Authority Representative or the EUC Citrix Supplier reserves the right to invoke a review of the Service Levels (including Service Level Targets) and KPIs;

25.5 Without prejudice to the provisions of the Change Control Procedure, the Supplier shall co-operate with any review of Service Levels undertaken in accordance with the provisions of paragraphs 23 and 24 The Supplier shall not unreasonably withhold agreement to the introduction of new Service Levels or the amendment of existing Service Levels.

25.6 Any change in Service Levels or associated Service Credits shall be subject to the Change Control Procedure.

25.7 Immediately following each anniversary of the Operational Services Commencement Date, the Supplier shall submit proposed improvements to the Service Levels (such as improved Service Level Targets) for the following 12 months in order to support the requirement for continuous improvements in its performance. These would be agreed between The Authority and the EUC Citrix Supplier.

25.8 If the Achieved Service Level does not meet the applicable Service Level Target, then Service Credits will be due from the Supplier in accordance with Paragraph 22.4

25.9 All Service Level Targets shall be measured over a Service Period, which unless otherwise specified in writing by The Authority, shall be a calendar month.

# 26. Service Credit Calculation

26.1 Service Credits will commence from 1st February 2019, unless otherwise agreed by both parties through the Contract Change Process.

26.2 These will be calculated as described within Clause 22.4

26.3 If the EUC Citrix Supplier provides their services against the agreed service definition and SLA, then the EUC Citrix Supplier will not be levied any Service Credits for non-performance of any applications or changes to Active Directory made by other 3rd parties that impact the Citrix Service.

26.4 In the event of repeat issues caused by the Authority’s IT Partners that impact the availability of the Citrix Service and that result in the EUC Citrix Partner having to expand significant time and effort, both Parties will discuss and agree the appropriate remediation steps to avoid repeat occurrence. Service Credits are a reduction of the amounts payable in respect of the Services and do not include VAT. The Supplier shall set-off the value of any Service Credits against the next appropriate invoice in accordance with the provisions of this Contract.

# 27. Service Levels Reporting And Management Information

27.1 For the Service Levels that apply to the EUC Citrix Services, and the KPIs that apply to the EUC Citrix Services, the EUC Citrix Supplier shall report on the measurement and management of these Service Levels and KPIs.

27.2 The EUC Citrix Supplier shall provide Management Information and Service Credit calculations in an aggregated form to The Authority based on its own records. The Management Information may include, but shall not be limited to, such of the following as The Authority Representative shall specify:

27.2.1 Availability of the ICT Services in the EUC Citrix Supplier’s scope;

27.2.2 Resolution targets for Incident management;

27.2.3 Resolution targets for service request management; and

27.2.4 Service Level Targets, or activities or tasks that make up a Request For Service.

27.3 The reports will only include the relevant Management Information when it occurs within a given month. This is in respect to the possible low incident rates related to the Citrix environment.

27.4 All Management Information and reports that are to be submitted to The Authority for a Service Period will be agreed between The Authority and the EUC Citrix Supplier.

# 28. Management and Escalation of Service Level Failures

28.1 Introduction

28.1.1 The procedures set out in this Section are intended to enable the Supplier to manage service issues arising from failure to achieve the Service Levels.

28.1.2 The Service Credit regime (as described in section 22) shall continue to apply throughout any escalation process.

28.1.3 The EUC Citrix Supplier shall proactively resolve outstanding issues relating to Services availability and performance and raise awareness of any matters that have, or may have, a material impact on the availability or performance of the Services.

28.1.4 Where further remedial action is required or where reasonably required by The Authority Representative, the EUC Citrix Supplier shall provide a Recovery Plan for the approval of the Authority Representative. The scope and format of all Recovery Plans shall be agreed with The Authority.

# 29. Supplier Management

29.1 The EUC Citrix Supplier shall work under the direction and management of the Service Management Supplier and shall comply with the Service Operations Manual in the operational delivery of the EUC Services.

29.2 The EUC Citrix Supplier shall support the Service Management Supplier in the development and maintenance of the Service Operations Manual to ensure that the EUC Services effectively interface with the ITIL processes and IT Services.

29.3 The EUC Citrix Supplier shall assist in addressing any non-compliance with the Service Operations Manual whether identified by the Service Management Supplier or otherwise.

29.4 The EUC Citrix Supplier shall work with the Service Management Supplier to develop and implement Operational Level Agreements and treat the Service Management Supplier and other IT Suppliers equally and impartially, and shall deal with the Service Management Supplier and IT Suppliers professionally, courteously and openly with the intention of achieving effective working relationships to deliver the best possible IT services.

29.5 The EUC Citrix Supplier shall continually monitor and optimise the EUC Services, related to the Citrix platform.

29.6 The EUC Citrix Supplier shall notify the Service Management Supplier as soon as they become aware of any issue or potential issue and provide proposals of how to address such issues.

29.7 The EUC Citrix Supplier shall provide information for the EUC Services and components thereof in accordance with the Service Operations Manual.

Where any major change may bring significant benefit to the buyer the Supplier will raise this for possible impact as a form Change for impacting and implementation.

# 30. Service Transition

## 30.1 Transition Planning and Support

30.1.1 The EUC Citrix Supplier shall provide Transition Services in line with the approach and plan submitted as part of the Suppliers tender documents.

30.1.2 The EUC Citrix Supplier shall support the Service Management

Supplier to assess risks to service failure and disruption through Transition and ensure that these have been understood and agreed with the Authority and that mitigating actions are in place with appropriate control and management in accordance with the Risk Management Policies and Procedures.

30.1.3 The EUC Citrix Supplier shall support the creation of Early Life Support Plans as directed by the Authority and shall address any issues identified by the Service Management Supplier through assurance of Early Life Support Plans

30.1.4 The EUC Citrix Supplier shall maintain the integrity of in situ EUC Service Assets, Configuration Items, Services and components thereof during the course of Transition and shall update the CMDB as necessary

30.1.5 The EUC Citrix Supplier shall update the CMDB and operational procedures as necessary to undertake effective management, delivery and support to the use and consumption of the new or changed EUC Services by the Authority.

## 30.2 Change and Evaluation Management

30.2.1 The EUC Citrix Supplier shall cater for all categories of EUC Change under the direction of the Service Management Supplier, including:

30.2.1.1 Operational Change requests;

30.2.1.2 Standard (pre-approved) Change requests e.g. via the Requestable Service Catalogue;

30.2.1.3 Emergency Change requests.

30.2.2 The EUC Citrix Supplier shall schedule, plan assess and implement Changes in accordance with the Service Operations Manual.

30.2.3 The EUC Citrix Supplier shall participate in Change Management

Board, Operational Change Advisory Board, and Post

Implementation Reviews in accordance with the Service Operations

Manual and as appropriate to the Citrix EUC management function

30.2.4 The EUC Citrix Supplier shall assess the impact of Changes on the EUC Services including:

30.2.4.1 Verified Implementation Plans;

30.2.4.2 Post Implementation Review;

30.2.4.3 Acceptance Criteria;

30.2.4.4 Back Out Plans or Remediation Plans;

30.2.4.5 Plans for handover to support.

30.2.5 The EUC Citrix Supplier shall update the CMDB and all relevant documentation in respect of all EUC Service Assets and

Configuration Items included in a Change as part of the execution of a Change, in accordance with the Service Operations Manual and such that the CMDB is at all times, an accurate reflection of the physical and logical implementation of the Services. This will only be in relation to the scope of the Citrix platform service provision.

30.2.6 Where any Change is simply not implementable without impact to

day to day support, based on its size and effort required, this will be costed and impacted as a formal Change.

30.2.7 The EUC Citrix Supplier shall implement all approved Changes; and shall not implement Changes that have not been properly authorised in accordance with the Service Operations Manual.

## 30.3 Knowledge Management

30.3.1 The EUC Citrix Supplier shall maintain and regularly update the Knowledge Database with Supplier solutions and best practices as they are developed, including updates based on “lessons learned”. 30.3.2 The EUC Citrix Supplier shall update a Service Knowledge

Management System (SKMS) in collaboration with the Service Management Supplier with data and information on the EUC Services including but not limited to:

30.3.2.1 Methods to resolve Incidents;

30.3.2.2 Known Errors;

30.3.2.3 Service Desk scripts;

30.3.2.4 Self-help articles; and

30.3.2.5 Frequently asked questions (FAQs). This will be stored in the Authority’s instance of ServiceNow.

30.3.3 When data relating to the EUC Services is found in the SKMS that is inaccurate, incomplete or lacks integrity, the EUC Citrix Supplier shall correct or remove such data, where it relates to the Citrix service 30.3.4 The EUC Citrix Supplier shall cooperate with the Service Management Supplier and the Authority to carry out conformance reviews and audits from time to time to ensure the integrity and accuracy of data in the SKMS.

## 30.4 Release and Deployment Management

30.4.1 The EUC Citrix Supplier shall under the direction of the Service Management Supplier provide input as required into all Release activities for the EUC elements relating to the Citrix platform, including but not limited to:

30.4.1.1 Release Plans;

30.4.1.2 Release Packages; 30.4.1.3 Implementation activities.

## 30.5 Service Asset and Configuration Management

30.5.1 The EUC Citrix Supplier shall work with the Service Management

Supplier to ensure that the CMDB provides a single view of Configuration Items, related to the Citrix environment being supported.

30.5.2 The EUC Citrix Supplier shall manage the identification, recording and maintenance of attributes of and relationships between Configuration Items (CIs) under the management of the EUC Citrix Supplier, including relationships to Configuration Items that are managed by other IT Suppliers, and shall update the CMDB

whenever changes to EUC CI's, within scope of the Citrix

Environment, or any of their attributes are made providing the CMDB implemented is deemed fit for purpose.

## 30.6 Service Validation and Testing

30.6.1 The EUC Citrix Supplier shall participate in Testing for EUC elements, related to the scope of the Citrix management provision, as directed by the Authority including Integration Testing, Operational Acceptance Testing and Service Acceptance Testing.

30.6.2 At the time of Contract signature there is no dedicated Citrix Test

environment, however, it is expected that the future target Cloud environment will provide the facility to create ‘on demand’ Test Environment/s.

30.6.3 For any project activity or significant Change if such Testing will impact day to day support and SLA achievement this will be flagged and subject to impact analysis.

# 31. Service Operations

## 31.1 Access Management

31.1.1 The EUC Citrix Supplier shall manage access to the IT Services through the Active Directory (SSO and MetaDirectory) Service. For the avoidance of doubt other IT Suppliers shall provide password management and user account creation services. The EUC Citrix Supplier is not responsible for Active Directory.

31.1.2 The EUC Citrix Supplier shall provide access to the Citrix Services in accordance with the User Administration Policy and the Service Operations Manual.

## 31.2 Event Management

31.2.1 The EUC Citrix Supplier shall log, track, filter, aggregate and associate EUC Events in accordance with the Service Operations Manual and shall provide automated alarms and indication of Incidents to the Service Management Supplier when thresholds are exceeded. This will need to be finalised as a part of the monitoring implementation solution, still to commence and be agreed with The Authority.

31.2.2 The EUC Citrix Supplier shall investigate in conjunction with the Service Management Supplier and other IT Suppliers the resolution of exceptional or abnormal Events that have reached a threshold or met certain criteria in accordance with the Service Operations Manual.

31.2.3 The EUC Citrix Supplier shall support the Service Management Supplier in the determination of EUC Event thresholds and shall set and adjust Event thresholds as directed by the Service Management Supplier.

## 31.3 Incident Management

31.3.1 The EUC Citrix Supplier shall investigate and resolve Incidents allocated to it by the Service Management Supplier in accordance with the Service Levels, including:

31.3.1.1 replace or repair faulty equipment, as appropriate, to the Citrix environment;

31.3.1.2 power-up and carry out scripted function testing, related to the Citrix platform

31.3.1.3 restore the equipment to its appropriate configuration, related to the Citrix environment;

31.3.1.4 test the replaced or repaired equipment to ensure it is functioning correctly, related to the Citrix platform

31.3.2 The EUC Citrix Supplier shall notify the Service Management Supplier promptly of any Incident of which it becomes aware of, other than through allocation from the Service Management Supplier.

31.3.3 The EUC Citrix Supplier shall proactively notify the Service

Management Supplier of any Incident that is known to be in breach or highly likely to create a P1 or P2 or that has, in the opinion of the EUC Citrix Supplier, been incorrectly allocated.

31.3.4 The EUC Citrix Supplier shall update the Incident record with all relevant information relating to the Incident and shall update Known Error information in the SKMS in relation to Incidents.

31.3.5 The EUC Citrix Supplier shall launch further investigation and action as required in relation to Incident trends.

## 31.4 Problem Management

31.4.1 The EUC Citrix Supplier shall provide a Problem Management Service that proactively seeks to prevent Incidents from happening within the EUC Services, and minimise the impact of Incidents that cannot be prevented.

31.4.2 The EUC Citrix Supplier shall analyse, monitor, progress, resolve and review Problems in line with the Service Levels and the Service Operations Manual, related to the Citrix service provisioned

31.4.3 The EUC Citrix Supplier shall provide Problem analysis and management information to the Service Management Supplier including, but not limited to, information relating to Problem trends, volumes and Problem solutions.

## 31.5 Service Request Fulfilment

31.5.1 The EUC Citrix Supplier shall fulfil Service Requests allocated to it by the Service Management Supplier in accordance with the Service Levels, including identifying and notifying the Service Management Supplier of any Service Requests that require Authority approval or action, raising of supplementary tasks or Change Requests, creation of Projects, or raising of Contract Changes.

31.5.2 The EUC Citrix Supplier shall respond to enquiries regarding Service Requests with accurate and up-to-date information.

31.5.3 The EUC Citrix Supplier shall provide early notification of any potential breach of Service Levels relating to P1 or P2 Service Requests to the Service Management Supplier.

31.5.4 The EUC Citrix Supplier shall provide to the Service Management

Supplier accurate and up-to-date management information regarding Service Requests including but not limited to volumes, trends and categories within each Service Reporting Period.

31.5.5 The EUC Citrix Supplier shall proactively monitor Service Requests to ensure that multiple and/or linked Service Requests are fulfilled in the most expedient and efficient manner to minimise business disruption.

## 31.6 Continual Service Improvement

31.6.1 Identify and Deliver Service Improvements

31.6.2 The EUC Citrix Supplier shall identify and notify to the Service Management Supplier process improvements and recommendations for consideration in respect of the EUC Services.

31.6.3 The EUC Citrix Supplier shall through continual improvement and by working together with the Service Management Supplier and other IT Suppliers and the Authority manage the reduction in volume of Incidents and Problems over the Term.

31.6.4 The EUC Citrix Supplier shall produce, maintain and provide to the Service Management Supplier a EUC Service Improvement Plan in accordance with the Service Operations Manual.

31.6.5 The EUC Citrix Supplier shall deliver service improvements under the

direction of the Service Management Supplier acting on behalf of the Authority in accordance with the agreed EUC Service Improvement Plan and shall keep the Service Management Supplier informed on the progress against Service Improvement Plans

31.6.6 The EUC Citrix Supplier shall provide advice, guidance and support to the Service Management Supplier on the use of the Services.

31.6.7 The EUC Citrix Supplier shall identify opportunities to improve the maturity of the EUC Services and their integration into the IT Services and shall manage the implementation of opportunities approved by the Service Management Supplier.

## 31.7 Service Management and Performance Management

31.7.1 The EUC Citrix Supplier shall measure, manage and report on the performance of the Citrix Services and the defined Service Levels in a monthly report to The Authority.

31.7.2 The EUC Citrix Supplier shall ensure performance information provided shall contain, but is not limited to, details of

31.7.2.1 performance over the agreed Service Reporting Period;

31.7.2.2 provide details of service credits accrued during the Service Reporting Period separately;

31.7.2.3 year to date; and

31.7.2.4 show an aggregate of performance month on month over a 12-month period.

31.7.3 The EUC Citrix Supplier shall ensure the quality of source information for performance is complete, accurate and timely

# 32. Service Lifecycle Management

## 32.1 IT Service Management Toolset (ITSM)

32.1.1 At the time of contract signature there is no integration between the

Authority’s and EUC Citrix Supplier’s ITSM toolsets.

32.1.2 The EUC Citrix Supplier has stated that they have plans to implement their own instance of ServiceNow. That being the case, both parties have agreed that it would be desirable to integrate both instances.

32.1.3 Any such integration will be handled via Contract Change Control and upon implementation, the EUC Citrix Supplier shall integrate its data, tools and processes with the ITSM Toolset (ServiceNow) provided by the Authority, in order to facilitate the efficient and timely delivery of the IT Services, including:

32.1.3.1 Availability Management Information System (AMIS)

32.1.3.2 IT Capacity Management Information System (CMIS)

32.1.3.3 Service Knowledge Management System (SKMS)

32.1.3.4 Event Management System

32.1.3.5 Incident Management System

32.1.3.6 Problem Management System

32.1.3.7 Authority Service Catalogue

32.1.3.8 Change Management

32.1.3.9 Configuration Management Database (CMDB)

32.1.4 The EUC Citrix Supplier shall comply with the ITSM Toolset’s Integration Standards and the Policies and Procedures for the maintenance, interfacing and update of the ITSM Toolset provided by the Authority

## 32.2 License Management and Compliance

32.2.1 The EUC Citrix Supplier shall manage the licensing for the tools they use to deliver the Citrix service, as requested within this document. The Authority will be responsible for the Citrix licensing used within their platform and by their users.

32.2.2 The EUC Citrix Supplier shall utilise the licences in the most costeffective manner available, while considering the business requirements.

## 32.3 Authority Business Security Requirements

32.3.1 The EUC Citrix Supplier and the Citrix Services shall comply with:

32.3.1.1 HMG Security Policy Framework (aligned with ISO 27001, found at

[https://www.gov.uk/government/publications/security-policyframework)](https://www.gov.uk/government/publications/security-policy-framework)

32.3.1.2 PSN Code of Connection (PSN CoCo) found at <https://www.gov.uk/public-services-network>

32.3.2 The EUC Citrix Supplier shall be able to communicate, store, transfer and process data on platforms accredited to handle the appropriate impact level associated with the EUC Services. EUC services are required to securely hold data at an Official – Sensitive level.

32.3.3 The EUC Citrix Supplier shall comply with the available Information Security Audit policies, procedures and compliance criteria.

32.3.4 The EUC Citrix Supplier shall support the Service Management Supplier to conduct Information Security Audits at least annually in line with the Authority processes, procedures and compliance criteria for the Citrix Services.

32.3.5 The EUC Citrix Supplier shall produce and maintain compliance statements and supporting documentary evidence in line with the obligations documented in any code of connections.

32.3.6 The EUC Citrix Supplier shall make available to the Authority any code of connection compliance report at least annually.

## 32.4 3rd Party Service Security

32.4.1 The Supplier shall support The Authority to ensure that EUC Citrix Environment is configured appropriately and can support the Authority’s approved Remote Access Security solution.

## 32.5 Investigation Support

32.5.1 In providing the Investigation Support Service the EUC Citrix Supplier shall:

32.5.1.1 comply with the requirements and standards set-out in the

Authority’s forensic readiness policy;

32.5.1.2 maintain information sufficient to support investigations in progress and provide processes and tools to assist the Authority in preserving digital evidence. This should be viewed in relation to recommendations within the Risk Register related to this service.

32.5.1.3 support and assist with digital forensic investigation activities

resulting from information leaking, fraud, disciplinary issues, inappropriate behaviour, accidents and negligence, commercial disputes and identity theft.

32.5.1.4 gather and provide information to support investigation activities;

32.5.1.5 ensure that such services can be carried out in such a manner as to minimise the impact to the Services – for the avoidance of doubt the Service Levels shall continue to apply during the course of any investigation activities;

32.5.1.6 hold evidence that can be reasonably provided for the Contract Period or as directed by the Authority of full audit records of investigation activities, securely and confidentially, and produce these on request to the Authority.

32.5.2 The EUC Citrix Supplier shall provide input and support the Authority in the delivery of Information Security Audits.

# 33. Security Monitoring and Alerting

33.1 The EUC Citrix Supplier will propose options for enhanced security monitoring and alerting as part of a future CSIP proposal.

1. For all the above scope it is stated within the context of the provision of Citrix services to the Authority, not any wider services. So, for example any DR requirement relates to the provision of EUC Citrix services, not the Authority’s wider services.

1. For any stated scope it is assumed that the solution is technically feasible to implement by the provided tools or in line with the stated policy. If a policy

defines something is not technically feasible to implement with the available tools, then this would be subject to discussion and impact with the Authority.

1. It is assumed that the existing documentation set, related to the Citrix platform, which will be provided by the incumbent partner, will be utilised and uplifted where required.

**Appendix 2**

**Contract Price**

# 37. Contract Cost Information

Below are the costs related to the transition of this service and the ongoing support:

37.1 **Transition Phase:**

*Redacted*

Notes

1. these costs will relate to the first phase of remediation tasks, which are called out within the table Risk Register in Section 38. This will be to execute those remediation tasks, working with the appropriate partners.

37.2 **Reoccurring Support:**



Notes

1. The support costs are based on a minimum 3 year contract period, whether the environment is within SCC Sentinel or Microsoft Azure platforms.
2. There will be a minimum 90 day cancellation period for this contract.
3. Application packaging is not a standard element of the support costs. However, we can manage this under change control, where and when required.
4. In regard to strategic advice these costs will be excluded for the existing platform, until the transition to the cloud platform begins. The costs will then transfer into a revised contract, which will be managed via the change control process

# 38. Risk Register

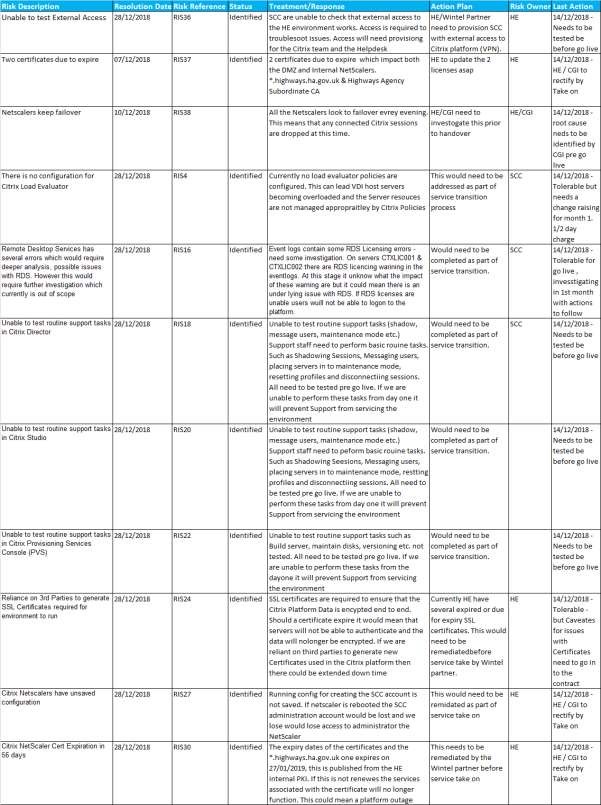
38.1 During the initial contract phase (month 1, wherever possible) we will need to resolve an initial tranche of risks within the risk register. These will include

resolution of two certificates, which are due to expire during January 2019. These represent a serious business impact to the delivery of the Citrix service for The Authority and need to be addressed urgently. Below, we have set out a summarised table of the tier 1 risks, which need to be resolved/initiated during the transition phase, wherever possible. We have also embedded the full risk register directly below, which details a 2nd tranche of month 2 risks or Service Improvements, which are not costed within our transition costs, but will be when we raise the appropriate change:



Copy of HE Risk

Register 17-12-18 v5



**Additional Services**

# A1 Transition to Cloud

As requested, below we have provided a rough estimate of the costs that would be required for the Supplier to transition the supported Citrix environment into a Cloud Based Environment.

The Supplier will provide analysis of the potential Cloud environments for the Citrix environment, and provide a recommendation of the best value-for-money environment for the Authority. This is to include, but not limited to the Authority’s Azure environment and he Microsoft/Citrix Azure environment.

*Redacted*

1. The transition to Azure includes a design phase. The Supplier will also need to ensure that the existing platform, is compliant with the Azure platform requirements. 2. These costs do not include any Azure platform costs or connectivity costs, including Express Route. Within the design phase of the transition to an Azure platform, the Supplier would look at the costs of the Azure platform. However the

Authority already has an Azure presence, which we’d propose to use and the associated cost model would be used by the Supplier to calculate the monthly costs for this.

3. Using Citrix best practise initial costs are calculated using an estimate of 35 x

VM’s, based on a user base of 800 x users to estimate the transition costs. These numbers were used as the Suppliers’ guidelines in achieving the estimated costs. 4. The Supplier are also assuming that the existing HE Active Directory can be reused for this project.

5. The costs suggested above are also subject to the completion of the Discovery phase and the implementation of the ‘must do’ remediation tasks. However, this could adjust the costs in either direction, up and down.

# A2 Investigating Citrix as a Security Vulnerability Mitigation

A security audit was undertaken in May 2017 which identified a number of applications hosted in The Authority’s data centres which had security vulnerabilities around the use of unsupported software i.e. Microsoft Server 2003 and Visual Basic Ver 6.

These applications are not scheduled for migration to Azure until Phase 2 or later, sometime in Q2 2019 or thereafter.

Thus, there remains a need to address security vulnerabilities in the interim. One possible avenue may be to utilise a Citrix secure environment to provide a whitelisted layer of access to the applications, limited only to specifically identified users.

The Supplier will produce a design for the utilisation of the Citrix secure environment to provide a white-listed layer of access to the applications, limited only to specifically identified users. This is for the purpose of addressing security vulnerabilities in the identified applications.

The Supplier will investigate the various technical implementations of Citrix and associated licencing models (including Citrix as a Service and hosting Citrix within Azure) to identify an approach and develop a design that best fits with HE requirements, and aligns to the Transition in A1.

**Schedule 3 Call Off Terms and Conditions**

**Information and Data Provisions**

1. **Confidentiality** 
   1. In respect of any Confidential Information it may receive directly or indirectly from the other

Party (“**Discloser**”) and subject always to the remainder of Clause 1 of this Schedule 3 of these Call-off Terms and Conditions, each Party (“**Recipient**”) undertakes to keep secret and strictly confidential and shall not disclose any such Confidential Information to any third party without the Discloser’s prior written consent provided that:

* + 1. the Recipient shall not be prevented from using any general knowledge, experience or skills which were in its possession prior to the Commencement Date;
    2. the provisions of Clause 1 of this Schedule 3 of these Call-off Terms and Conditions shall not apply to any Confidential Information:
       - 1. which is in or enters the public domain other than by breach of this Contract or other act or omissions of the Recipient;
         2. which is obtained from a third party who is lawfully authorised to disclose such information without any obligation of confidentiality;
         3. which is authorised for disclosure by the prior written consent of the Discloser;
         4. which the Recipient can demonstrate was in its possession without any obligation of confidentiality prior to receipt of the Confidential Information from the Discloser; or
         5. which the Recipient is required to disclose purely to the extent to comply with the requirements of any relevant stock exchange.
  1. Nothing in Clause 1 of this Schedule 3 of these Call-off Terms and Conditions shall prevent the Recipient from disclosing Confidential Information where it is required to do so by judicial, administrative, governmental or regulatory process in connection with any action, suit, proceedings or claim or otherwise by applicable Law, including the Freedom of Information Act

2000 (“**FOIA**”), Codes of Practice on Access to Government Information, on the Discharge of Public Authorities’ Functions or on the Management of Records (“**Codes of Practice**”) or the Environmental Information Regulations 2004 (“**Environmental Regulations**”).

* 1. The Authority may disclose the Supplier’s Confidential Information:
     1. on a confidential basis, to any Contracting Authority (the Parties agree that all Contracting Authorities receiving such Confidential Information shall be entitled to further disclose the Confidential Information to other Contracting Authorities on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Contracting Authority);
     2. on a confidential basis, to any consultant, contractor or other person engaged by the Authority and/or the Contracting Authority receiving such information;
     3. to any relevant party for the purpose of the examination and certification of the Authority’s accounts;
     4. to any relevant party for any examination pursuant to section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;
     5. to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirements; or
     6. on a confidential basis, to a proposed successor body in connection with any

proposed or actual, assignment, novation or other disposal of rights, obligations, liabilities or property in connection with this Contract;

and for the purposes of this Contract, references to disclosure "on a confidential basis" shall mean the Authority making clear the confidential nature of such information and that it must not be further disclosed except in accordance with Law or this Clause 1.3 of this Schedule 3 of these Call-off Terms and Conditions. .

* 1. The Supplier may only disclose the Authority’s Confidential Information, and any other information provided to the Supplier by the Authority in relation to this Contract, to the Supplier’s Staff or professional advisors who are directly involved in the performance of or advising on the Supplier’s obligations under this Contract. The Supplier shall ensure that such Staff or professional advisors are aware of and shall comply with the obligations in Clause 1 of this Schedule 3 of these Call-off Terms and Conditions as to confidentiality and that all information, including Confidential Information, is held securely, protected against unauthorised use or loss and, at the Authority’s written discretion, destroyed securely or returned to the Authority when it is no longer required. The Supplier shall not, and shall ensure that the Staff do not, use any of the Authority’s Confidential Information received otherwise than for the purposes of performing the Supplier’s obligations in this Contract.
  2. For the avoidance of doubt, save as required by Law or as otherwise set out in this Schedule 3 of these Call-off Terms and Conditions, the Supplier shall not, without the prior written consent of the Authority (such consent not to be unreasonably withheld or delayed), announce that it has entered into this Contract and/or that it has been appointed as a Supplier to the Authority and/or make any other announcements about this Contract.
  3. Clause 1 of this Schedule 3 of these Call-off Terms and Conditions shall remain in force:
     1. without limit in time in respect of Confidential Information which comprises Personal Data or which relates to national security; and
     2. for all other Confidential Information for a period of three (3) years after the expiry or earlier termination of this Contract unless otherwise agreed in writing by the Parties.

1. **Data protection** 
   1. The Parties acknowledge their respective duties under Data Protection Legislation and shall give each other all reasonable assistance as appropriate or necessary to enable each other to comply with those duties. For the avoidance of doubt, the Supplier shall take reasonable steps to ensure it is familiar with the Data Protection Legislation and any obligations it may have under such Data Protection Legislation and shall comply with such obligations.
   2. Where the Supplier is Processing Personal Data under or in connection with this Contract, the Parties shall comply with the Data Protection Protocol.
   3. The Supplier and the Authority shall ensure that Personal Data is safeguarded at all times in accordance with the Law, and this obligation will include (if transferred electronically) only transferring Personal Data (a) if essential, having regard to the purpose for which the transfer is conducted; and (b) that is encrypted in accordance with any international data encryption standards for healthcare, and as otherwise required by those standards applicable to the Authority under any Law and Guidance (this includes, data transferred over wireless or wired networks, held on laptops, CDs, memory sticks and tapes).
   4. Where, as a requirement of this Contract, the Supplier is Processing Personal Data relating to patients and/or service users as part of the Services, the Supplier shall:
      1. complete and publish an annual information governance assessment using the NHS information governance toolkit;
      2. achieve a minimum level 2 performance against all requirements in the relevant NHS information governance toolkit;
      3. nominate an information governance lead able to communicate with the Supplier’s board of directors or equivalent governance body, who will be responsible for information governance and from whom the Supplier’s board of directors or equivalent governance body will receive regular reports on information governance matters including, but not limited to, details of all incidents of data loss and breach of confidence;
      4. report all incidents of data loss and breach of confidence in accordance with Department of Health and/or the NHS England and/or Health and Social Care Information Centre guidelines;
      5. put in place and maintain policies that describe individual personal responsibilities for handling Personal Data and apply those policies vigorously;
      6. put in place and maintain a policy that supports its obligations under the NHS Care Records Guarantee (being the rules which govern information held in the NHS Care Records Service, which is the electronic patient/service user record management service providing authorised healthcare professionals access to a patient’s integrated electronic care record);
      7. put in place and maintain agreed protocols for the lawful sharing of Personal Data with other NHS organisations and (as appropriate) with non-NHS organisations in circumstances in which sharing of that data is required under this Contract;
      8. where appropriate, have a system in place and a policy for the recording of any telephone calls in relation to the Services, including the retention and disposal of those recordings;
      9. at all times comply with any information governance requirements and/or processes as may be set out in the Specification and Tender Response Document; and
      10. comply with any new and/or updated requirements, Guidance and/or Policies notified to the Supplier by the Authority from time to time (acting reasonably) relating to the Processing and/or protection of Personal Data.
   5. Where any Personal Data is Processed by any Sub-contractor of the Supplier in connection with this Contract, the Supplier shall procure that such Sub-contractor shall comply with the relevant obligations set out in Clause 2 of this Schedule 3 of these Call-off Terms and Conditions, as if such Sub-contractor were the Supplier.
   6. The Supplier shall indemnify and keep the Authority indemnified against, any loss, damages, costs, expenses (including without limitation legal costs and expenses), claims or proceedings whatsoever or howsoever arising from the Supplier’s unlawful or unauthorised Processing, destruction and/or damage to Personal Data in connection with this Contract.
2. **Freedom of Information and Transparency** 
   1. The Parties acknowledge the duties of Contracting Authorities under the FOIA, Codes of Practice and Environmental Regulations and shall give each other all reasonable assistance as appropriate or necessary to enable compliance with those duties.
   2. The Supplier shall assist and cooperate with the Authority to enable it to comply with its disclosure obligations under the FOIA, Codes of Practice and Environmental Regulations. The Supplier agrees:
      1. that this Contract and any recorded information held by the Supplier on the

Authority’s behalf for the purposes of this Contract are subject to the obligations and commitments of the Authority under the FOIA, Codes of Practice and Environmental Regulations;

* + 1. that the decision on whether any exemption to the general obligations of public access to information applies to any request for information received under the FOIA, Codes of Practice and Environmental Regulations is a decision solely for the Authority;
    2. that where the Supplier receives a request for information under the FOIA, Codes of Practice and Environmental Regulations and the Supplier itself is subject to the FOIA, Codes of Practice and Environmental Regulations it will liaise with the Authority as to the contents of any response before a response to a request is issued and will promptly (and in any event within two (2) Business Days) provide a copy of the request and any response to the Authority;
    3. that where the Supplier receives a request for information under the FOIA, Codes of Practice and Environmental Regulations and the Supplier is not itself subject to the FOIA, Codes of Practice and Environmental Regulations, it will not respond to that request (unless directed to do so by the Authority) and will promptly (and in any event within two (2) Business Days) transfer the request to the Authority;
    4. that the Authority, acting in accordance with the Codes of Practice issued and revised from time to time under both section 45 of FOIA, and regulation 16 of the Environmental Regulations, may disclose information concerning the Supplier and this Contract; and
    5. to assist the Authority in responding to a request for information, by processing information or environmental information (as the same are defined in FOIA and the Environmental Regulations) in accordance with a records management system that complies with all applicable records management recommendations and codes of conduct issued under section 46 of FOIA, and providing copies of all information requested by the Authority within five (5) Business Days of that request and without charge.
  1. The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, Codes of Practice and Environmental Regulations, the content of this Contract is not Confidential Information.
  2. Notwithstanding any other term of this Contract, the Supplier consents to the publication of this Contract in its entirety (including variations), subject only to the redaction of information that is exempt from disclosure in accordance with the provisions of the FOIA, Codes of Practice and Environmental Regulations.
  3. In preparing a copy of this Contract for publication under Clause 3.4 of this Schedule 3 of these Call-off Terms and Conditions, the Authority may consult with the Supplier to inform decision making regarding any redactions but the final decision in relation to the redaction of information will be at the Authority’s absolute discretion.
  4. The Supplier shall assist and cooperate with the Authority to enable the Authority to publish this Contract.
  5. Where any information is held by any Sub-contractor of the Supplier in connection with this Contract, the Supplier shall procure that such Sub-contractor shall comply with the relevant obligations set out in Clause 3 of this Schedule 3 of these Call-off Terms and Conditions, as if such Sub-contractor were the Supplier.

1. **Information Security** 
   1. Without limitation to any other information governance requirements set out in this Schedule 3 of these Call-off Terms and Conditions, the Supplier shall:
      1. notify the Authority forthwith of any information security breaches or near misses (including without limitation any potential or actual breaches of confidentiality or actual information security breaches) in line with the Authority’s information governance Policies; and
      2. fully cooperate with any audits or investigations relating to information security and any privacy impact assessments undertaken by the Authority and shall provide full information as may be reasonably requested by the Authority in relation to such audits, investigations and assessments.
   2. Where required in accordance with the Specification and Tender Response Document, the Supplier will ensure that it puts in place and maintains an information security management plan appropriate to this Contract, the type of Services being provided and the obligations placed on the Supplier. The Supplier shall ensure that such plan is consistent with any relevant Policies, Guidance, Good Industry Practice and with any relevant quality standards as may be set out in the Key Provisions and/or the Specification and Tender Response Document.
   3. Where required in accordance with the Specification and Tender Response Document, the Supplier shall obtain and maintain certification under the HM Government Cyber Essentials Scheme at the level set out in the Specification and Tender Response Document.

**Appendix 3 DATA PROTECTION PROTOCOL**

**Table A – Processing, Personal Data and Data Subjects**

|  |  |
| --- | --- |
| **Description** | **Details** |
| Subject matter of the Processing | Data processing will relate to ICT EUC Citrix Environment and the EUC Citrix services, and should be limited to information required to perform those services, including the location of a user (whether an office location or in the case of a home worker, a home address). |
| Duration of the Processing | The data processing will commence from the commencement date of this contract, 11th January 2019, for a period of two years. This may be extended by up two years. Data processing will cease on the expiry of the contract. |
| Nature and purposes of the Processing | The data will contain information required to identify individual Authority users, including their location (either an office location or in the case of a home worker, a home address). This is to enable the Supplier to provide the EUC Citrix Service to the user, and enable them to use their IT services. |
| Type of Personal Data | Name  Authority IT User Name  Address  Telephone Number |
| Categories of Data Subject | The data subjects will be Authority staff (including contractors, agents and temporary workers) |
| 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 | Personal data should be kept by the Supplier for processing until the relevant task that requires the data has been closed and accepted by the Authority. On expiry of the contract (maximum of 4 years), data will be returned to the Authority, and Supplier copies destroyed. |

data

**Definitions**

The definitions and interpretative provisions at Schedule 4 (Definitions and Interpretations) of the Contract shall also apply to this Protocol. Additionally, in this Protocol the following words shall have the following meanings unless the context requires otherwise:

|  |  |
| --- | --- |
| **“Data Loss Event”** | means any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of  Personal Data in breach of this Contract, including any Personal  Data Breach**;** |
| “**Data Protection Impact**  **Assessment**” | means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data; |
| “**Data Protection Officer**” and  **“Data Subject**” | shall have the same meanings as set out in the GDPR; |
| “**Data Subject Access Request”** | means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data. |
| “**Personal Data Breach**” | shall have the same meaning as set out in the GDPR; |
| “**Protective Measures”** | means appropriate technical and organisational measures which may include:pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it; |
| **“Protocol” or “Data Protection**  **Protocol”** | means this Data Protection Protocol; |
| “**Sub-processor”** | means any third party appointed to Process Personal Data on behalf of the Supplier related to this Contract. |

1. **DATA PROTECTION** 
   1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor. The only Processing that the Supplier is authorised to do is listed in Table A of this Protocol by the Authority and may not be determined by the Supplier.
   2. The Supplier shall notify the Authority immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.
   3. The Supplier shall provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Authority, include:
      1. a systematic description of the envisaged Processing operations and the purpose of the Processing;
      2. an assessment of the necessity and proportionality of the Processing operations in relation to the Services;
      3. an assessment of the risks to the rights and freedoms of Data Subjects; and
      4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
   4. The Supplier shall, in relation to any Personal Data Processed in connection with its obligations under this Contract:
      1. process that Personal Data only in accordance with Table A of this Protocol, unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Authority before Processing the Personal Data unless prohibited by Law;
      2. ensure that it has in place Protective Measures, which have been reviewed and approved by the Authority as appropriate to protect against a Data Loss Event having taken account of the:
         1. nature of the data to be protected;
         2. harm that might result from a Data Loss Event;
         3. state of technological development; and
         4. cost of implementing any measures;
      3. ensure that:
         1. the Supplier Personnel do not Process Personal Data except in accordance with this Contract (and in particular Table A of this Protocol);
         2. it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:
            1. are aware of and comply with the Supplier’s duties under this Protocol;
            2. are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;
            3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Authority or as otherwise permitted by this Contract; and
            4. have undergone adequate training in the use, care, protection and handling of Personal Data;
      4. not transfer Personal Data outside of the EU unless the prior written consent of the Authority has been obtained and the following conditions are fulfilled:
         1. the Authority or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the GDPR or Article 37 of the

Law Enforcement Directive (Directive (EU) 2016/680)) as determined by the Authority;

* + - 1. the Data Subject has enforceable rights and effective legal remedies;
      2. the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred

(or, if it is not so bound, uses its best endeavours to assist the Authority in meeting its obligations); and

* + - 1. the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the Processing of the Personal Data;
    1. at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination or expiry of the Contract unless the Supplier is required by Law to retain the Personal Data.
  1. Subject to Clause 1.6 of this Protocol, the Supplier shall notify the Authority immediately if it:
     1. receives a Data Subject Access Request (or purported Data Subject Access Request);
     2. receives a request to rectify, block or erase any Personal Data;
     3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
     4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Contract;
     5. receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
     6. becomes aware of a Data Loss Event.
  2. The Supplier’s obligation to notify under Clause 1.5 of this Protocol shall include the provision of further information to the Authority in phases, as details become available.
  3. Taking into account the nature of the Processing, the Supplier shall provide the Authority with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 1.5 of this Protocol (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:
     1. the Authority with full details and copies of the complaint, communication or request; 1.7.2 such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Access Request within the relevant timescales set out in the

Data Protection Legislation;

* + 1. the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;
    2. assistance as requested by the Authority following any Data Loss Event;
    3. assistance as requested by the Authority with respect to any request from the

Information Commissioner’s Office, or any consultation by the Authority with the Information Commissioner's Office.

* 1. The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Protocol. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:
     1. the Authority determines that the Processing is not occasional;
     2. the Authority determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
     3. the Authority determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
  2. The Supplier shall allow for audits of its Processing activity by the Authority or the Authority’s designated auditor.
  3. The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation.
  4. Before allowing any Sub-processor to Process any Personal Data related to this Contract, the Supplier must:
     1. notify the Authority in writing of the intended Sub-processor and Processing;
     2. obtain the written consent of the Authority;
     3. enter into a written agreement with the Sub-processor which give effect to the terms set out in this Protocol such that they apply to the Sub-processor; and
     4. provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.
  5. The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.
  6. The Authority may, at any time on not less than 30 Business Days’ notice, revise this Protocol by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract).
  7. The Parties agree to take account of any guidance issued by the Information Commissioner’s

Office. The Authority may on not less than 30 Business Days’ notice to the Supplier amend this Protocol to ensure that it complies with any guidance issued by the Information

Commissioner’s Office.

* 1. The Supplier shall comply with any further instructions with respect to Processing issued by the Authority by written notice. Any such further written instructions shall be deemed to be incorporated into Table A above from the date at which such notice is treated as having been received by the Supplier in accordance with Clause 27.2 of Schedule 2 of the Contract.
  2. Subject to Clauses 1.13, 1.14, and 1.15 of this Protocol, any change or other variation to this Protocol shall only be binding once it has been agreed in writing and signed by an authorised representative of both Parties.