Terms and conditions (Supplier Terms)

Health: Software as a Service (SaaS)

Structure of these Supplier Terms

These Supplier Terms contain provisions that are specific to the provision of Health SaaS. At the end of these Supplier Terms there are also a number of Annexes, which set out additional product/service specific provisions (which also override the General Provisions if there is any conflict). Only the Annexes which relate to the products/services purchased by the Buyer (as set out in the Particulars) shall apply. There are Annexes for:

- NEC Newborn Hearing Screening Programme S4H
- NEC Rego
- NEC OptoMize
- Abdominal Aortic Aneurysm (AAA) SMaRT SaaS
- NEC Registries as a Service.

At the end of these Supplier Terms is a Glossary. Any capitalised terms within these Supplier Terms which are not defined in the Glossary shall have the meaning set out elsewhere in this Agreement.

General Provisions

SaaS Onboarding Services

The Supplier shall deliver the SaaS Onboarding Services specified in the Particulars.

Unless expressly stated otherwise in the Particulars, the parties recognise that any SaaS Onboarding Services and Professional Service days set out in this Agreement are an estimate based on the parties' current understanding of their requirements and obligations.

Unless expressly stated otherwise in the Particulars, all SaaS shall be tested in accordance with the Supplier's standard test policies. Any additional testing activities that the Buyer requires the Supplier to carry out must be agreed in writing between the parties and may be chargeable. The Buyer shall be deemed to accept the SaaS, and such acceptance shall be irrevocable, if the SaaS is used by the Buyer in a live environment and/or for any live operations.

Access to and use of the SaaS

Subject to the Buyer complying with the restrictions set out in these Supplier Terms and the other terms and conditions of this Agreement, the Supplier shall grant to the Buyer a non-exclusive, non-transferable right to permit the Authorised Users to use the SaaS and the Documentation during the SaaS Term solely for the Buyer's internal business purposes.

The Supplier shall grant the Buyer's Administrator access to the SaaS in the technologically appropriate manner either by provision of a licence key, by granting access to a downloadable app, or by means of issuing a user name and password for the SaaS portal which can be accessed through such URL as may be notified by the Supplier from time to time ("**SaaS Portal**").

The Buyer's Administrator shall then be permitted to access the SaaS through the SaaS Portal and it shall be the Buyer's Administrator's responsibility to configure the set-up of the SaaS, within the parameters set out within the Documentation, to reflect the Buyer's own policies and practices on application assessment and decision making.

The Buyer's Administrator, in accordance with the Documentation, shall be permitted to set up further users authorised to access the SaaS on behalf of the Buyer. It is the Buyer's Administrator's responsibility to set the controls on and levels of access for each further user authorised. For the avoidance of doubt, the Buyer's Administrator and the further users set up by the Buyer's Administrator under this paragraph shall be the "Authorised Users" for the purposes of this Agreement.

If there is an End User named in the Particulars, the Supplier grants the Buyer the right to access and use the SaaS for the benefit of such End User.

In relation to the Authorised Users, the Buyer undertakes that:

- Each Authorised User shall keep a secure password for his/her use of the SaaS and Documentation, that such password shall be kept confidential and shall be changed no less frequently than every 90 days;
- It shall permit the Supplier to audit the SaaS. Such audit may be conducted no more than once per quarter, at the Supplier's expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with the Buyer's normal conduct of business; and

If any of the audits referred to in this paragraph reveal that any unauthorised access has occurred, then without prejudice to the Supplier's other rights, the Buyer shall promptly disable such accounts.

- In relation to the Buyer's Administrator, the Buyer undertakes that:
- The Buyer's Administrator will review and act upon any update information or reasonable instructions of the Supplier, including disseminating such applicable update information and instructions to other Authorised Users; and
- The Buyer's Administrator shall monitor the Authorised Users and ensure that they act in accordance with the terms of this Agreement.

The Buyer shall not (and shall ensure that its Authorised Users shall not) access, store, distribute or transmit any Viruses, or any material during the course of its use of the SaaS that:

- Is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;
- Facilitates illegal activity;
- Depicts sexually explicit images;
- Promotes unlawful violence;
- Is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or
- Is otherwise illegal or causes damage or injury to any person or property,

And the Supplier reserves the right, without liability or prejudice to its other rights to the Buyer, to disable the Buyer's access to any material that breaches the provisions of this paragraph.

The Buyer shall not (and shall ensure that its Authorised Users shall not):

- Attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the SaaS, except:
  - ➔ As may be allowed by any applicable law which is incapable of exclusion by agreement between the parties; and
  - ➔ To the extent expressly permitted under this Agreement.
- Attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the SaaS and/or Documentation (as applicable) in any form or media or by any means; or
- Access all or any part of the Services and Documentation in order to build a product or service which competes with the SaaS and/or the Documentation; or
- Use the SaaS and/or Documentation to provide services to third parties (the Buyer's citizens shall not be deemed to be third parties for the purposes of this paragraph); or
- License, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the SaaS and/or Documentation available to any third party except the Authorised Users; or
- Attempt to obtain, or assist third parties in obtaining, access to the SaaS and/or Documentation, other than as provided under this paragraph.

The Buyer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the SaaS and/or the Documentation and, in the event of any such unauthorised access or use, promptly notify the Supplier.

The Buyer shall access the SaaS by network communications as agreed between the parties.

The Supplier will use reasonable commercial endeavours to accommodate the introduction of legislative changes. The Supplier expressly reserves the right to charge for the provision of any such legislative updates where: (a) the development of the update is in the reasonable opinion of the Supplier technically complex; and (b) the costs of developing the update are in the reasonable opinion of the Supplier sufficient to warrant a charge for the provision of the update to the Supplier's buyers at large.

Security, Disaster Recovery and Back-up Policy

The Buyer shall own all right, title and interest in and to all of the Buyer Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Buyer Data.

The Supplier confirms that:

- The SaaS is provided via a private community cloud for the sole use by or on behalf of the public sector;
- The SaaS platform is designed and implemented in accordance with the 27001 baseline control set, the 14 Cloud Security Principles and National Cyber Security Centre (NCSC) guidance. The platform has a number of tenants that have undergone formal accreditations from various independent and Government departments. The environment from which the SaaS shall be delivered conforms to the relevant sections of the Government Security Policy Framework and

Personnel Security Controls and to all relevant Communications Electronics Security Group Memoranda, Manuals and Standards;

- It shall comply with the Supplier's Privacy and Security Policy relating to the privacy and security of the Buyer Data;
- Its information security management system is certified to ISO 27001 and ISO 27002;
- Its quality management system is certified to ISO 9001:2008 (TickIT);
- Its service management system operates in accordance with ITIL v.3; and
- The information assurance process as detailed within the paragraphs above will be periodically revised and updated to ensure alignment with good industry practice.

The Buyer recognises that the SaaS is a hosted, multi-tenanted solution. The Buyer Data will be segregated from the data of other Supplier buyers using the SaaS and there will be no data sharing facility unless expressly authorised by the Buyer.

The Supplier confirms that it uses more than one data centre with separate infrastructure and resilience for provision of the SaaS to ensure relocation of the SaaS provision in the event of non-availability of one data centre.

The Supplier confirms that its disaster recovery and business continuity policies, processes and procedures are based on standard BS25999 and ISO 22301:2019.

The Back-Up Policy is as follows:

- The Supplier takes multiple back-ups within the system as part of the SaaS, in particular, back-ups (using a cycle that includes daily (incremental), weekly (entire image), monthly and annual saves) are taken daily from the live system utilising an automated process scheduled to run overnight, taking into account any batch routines and system availability requirements;
- Back-ups are transferred offsite daily and stored in a secure offsite location;
- In the event of any loss or damage to Buyer Data, the Buyer's sole and exclusive remedy shall be for the Supplier to use reasonable commercial endeavours to restore the lost or damaged Buyer Data from the latest back-up of such Buyer Data maintained by the Supplier; and
- The Supplier shall not be responsible for any loss, destruction, alteration or disclosure of Buyer Data caused by any third party (except those third parties sub-contracted by the Supplier to perform services related to Buyer Data maintenance and back-up).

Buyer Obligations

Except where the Supplier has specifically agreed to provide such services the Buyer will:

- During the onboarding phase provide appropriately skilled personnel to support configuration of the SaaS, as required;
- Be responsible for the operation and use of the SaaS and any associated documentation and the results obtained from these; and
- Supply the Supplier with any information and assistance reasonably necessary for the Supplier to perform its obligations under this Agreement.

The Buyer shall in good faith:

- Provide the Supplier with (i) all necessary co-operation in relation to this Agreement; and (ii) all necessary access to such information as may be required by the Supplier in order to provide the SaaS, including but not limited to Buyer Data;
- Comply with all applicable laws and regulations with respect to its activities under this Agreement;
- Carry out all other Buyer responsibilities set out in this Agreement in a timely and efficient manner. In the event of any delays in the Buyer's provision of such assistance as agreed by the parties, the Supplier may adjust any agreed timetable or delivery schedule as reasonably necessary and reserves the right to charge the Buyer for any costs incurred by the Supplier as a consequence of such delay;
- Ensure that (where applicable) the Authorised Users use the SaaS and the Documentation in accordance with the terms and conditions of this Agreement and shall be responsible for any Authorised User's breach of this Agreement;
- Obtain and shall maintain all necessary licences, consents, and permissions necessary for the Supplier, its contractors and agents to perform their obligations under this Agreement, including without limitation the SaaS;
- Ensure that its network and systems comply with the relevant specifications provided by the Supplier from time to time; and
- To the extent it is within their control, be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to the Supplier's data centres, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Buyer's network connections or telecommunications links or caused by the internet. The Supplier is not responsible for network issues which arise outside of its network perimeter.

SaaS Availability and Support

The Supplier shall use commercially reasonable endeavours to make the SaaS available 08:00 to 20:00 UK time on Business Days, except for:

- Planned maintenance carried out during the maintenance window of (i) 17:30 to 09:00 UK time on Business Days; and (ii) at any time on a non-Business Day, for which the Supplier shall give the Buyer at least 24 hours' notice in advance; and
- Unscheduled emergency maintenance carried out, where possible unless there is an identified and demonstrable immediate risk to the SaaS infrastructure, during the maintenance window of (i) 17:30 to 09:00 UK time on a Business Day; and (ii) at any time on a non-Business Day, for which the Supplier shall use reasonable endeavours to give the Buyer at least six hours' notice in advance.

The SaaS supports mainstream browsers for example IE (until June 2022), Edge, Chrome, Firefox and Safari unless otherwise stated in the release documentation.

During the SaaS Term the Supplier shall, as part of the SaaS and at no additional cost to the Buyer, provide the Buyer with the Supplier's standard Buyer support services through its service desk ("**Service Desk**").

The Service Desk can be contacted by the Buyer's Authorised Users in the following ways during the following times:

- Via the Supplier's customer portal which can be accessed through the URL https://helphub.necsws.com/ ("**Customer Portal**"), 24 hours a day, seven days a week; or
- Where the Customer Portal is not available for any reason, through the Service Desk telephone number (to be provided) during Normal Business Hours.

When logging a request for support ("**Support Request**"), the Authorised User must provide the following information to the Service Desk (whether through the Customer Portal or via email):

- Authorised User Name;
- Authorised User Location;
- Authorised User's contact details – telephone and email;
- Details of the nature of the fault or description of the issue; and
- Details of who is being affected, i.e. single user, a group of users or the whole organisation, and the impact that the fault or issue is having including any urgency surrounding the support call.

The Service Desk will then resolve the call remotely, which may (a) involve a call to the Authorised User for additional information and data; and/or (b) referral to the Supplier's application support team for further investigation.

The Supplier shall have no obligation to:

- Correct any incident reported by the Buyer if such reported incident is not reproducible by the Supplier in the SaaS; or
- Correct any Priority 4 reported incident and reserves the right to abandon attempts to provide a fix where the costs are likely to be excessive or the commercial benefits to the Supplier's customers at large are likely to be negligible; or
- Correct any incident if such incident arises from misuse or abuse of the SaaS.

Termination and Consequences of Termination

In the event the Supplier elects to withdraw a particular type of SaaS, it may do so without liability provided it has given the Buyer not less than six months' prior written notice.

The Supplier shall, following the expiry of the SaaS Term, disable the Buyer's access to the SaaS.

Miscellaneous

- If this Agreement contains the Buyer's service description, requirements or specification ("**Specification**") and if any provision of that Specification conflicts with these Supplier Terms, then regardless of any other provision in this Agreement, these Supplier Terms will take precedence.
- Regardless of any other provision in this Agreement, except to the extent not permitted by law:

- The Buyer assumes sole responsibility for results obtained from its use of the Supplier's deliverables and for any conclusions drawn from such use; and
- The Supplier shall have no liability for any damage caused by errors or omissions in any information, data, instructions or scripts provided to the Supplier by the Buyer in connection with this Agreement, or any actions taken by the Supplier at the Buyer's direction.

- Except where the Supplier has specifically agreed to provide such services, the Buyer will promptly:
  - Supply the Supplier with any information and assistance reasonably necessary for the Supplier to perform its obligations under this Agreement; and
  - Provide the Supplier's personnel with full free and safe access to its site when required, to enable the Supplier to perform its obligations under this Agreement.
- The Buyer warrants, represents and undertakes to the Supplier that there will be no relevant transfer for the purposes of the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ("**TUPE**") of employees from the Buyer (or any supplier, contractor or other service provider to the Buyer) to the Supplier. Regardless of any other provision of this Agreement, the Buyer agrees to indemnify the Supplier against all costs, claims, liabilities and expenses (including reasonable legal expenses) incurred by the Supplier in connection with or as a result of:
  - A claim by any person who transfers or alleges that they have transferred to the Supplier as a result of entering into this Agreement; and/or
  - Any failure by the Buyer to comply with its obligations under regulations 13 and 14 of TUPE, or any award of compensation under regulation 15 of TUPE.

Annex: NEC Newborn Hearing Screening Programme S4H

The additional provisions set out in this Annex apply to the provision of NEC Newborn Hearing Screening Programme S4H Software as a Service ("**S4H SaaS**"). If there is any conflict between the provisions set out in this Annex and the General Provisions, this Annex shall apply.

These provisions are relevant to all NHS and Approved Screening Service providers of the England, Wales, Scotland and Northern Ireland Newborn Hearing Screening ("**NHSP**") Screening Programmes. S4H SaaS is accessible to all authorised NHS users for the purposes of supporting the UK (Great Britain and Northern Ireland) National NHSP Screening Programme. Users need to be connected to the HSCN / SWAN Network.

Technical Requirements

Service Dependencies

In order to access and use the S4H SaaS the Buyer must provide the following:

- An HSCN / Swan Network connection to access S4H SaaS.
- Bandwidth and Latency Requirements
- S4H SaaS is designed to work over a range of bandwidths, dependent on the number of users, and the type of data to be uploaded / displayed. As a minimum HSCN/ SWAN Network throughput speeds for the Buyer site must be 256kb/s or above.

Backup / Restore

The Supplier will ensure Buyer Data is backed up daily from the live systems using an automated process scheduled to run overnight, taking into account any batch routines and service availability requirements.

The backup tape cycle includes:

- Daily (incremental)
- Weekly (entire image)
- Monthly and annual saves.

Backup tapes are taken off-site daily and stored in a secure location. S4H SaaS is delivered from two data centres. Each has a physically separate infrastructure, such that a failure in one will not affect another.

Inter-data centre connectivity provides telecommunications resilience and data replication. All production critical data is replicated to the secondary data centre.

The primary data centre has been designed to be highly resilient to meet requirements for performance and availability. All components have in-built redundancy (for example, multiple power supplies, fans, and so on), with components deployed in duplicate in either an active-active or fail-over configuration.

Disaster Recovery

The Supplier confirms that its disaster recovery and business continuity policies, processes and procedures are based on standard BS25999 and ISO 22301:2019.

These support an ITIL IT service continuity management function.

Service Level Agreement

For the purposes of this Service Level Agreement, the following terms shall have the meaning set out below:

Core Service Hours means 9.00am to 5.00pm Monday to Friday excluding bank holidays in England and Wales.

Service Availability

The Supplier provides S4H SaaS as a fully hosted and supported solution. The Supplier shall use commercially reasonable endeavours to make the service available 24x7x365 subject to downtime for routine and emergency maintenance.

Help Desk

Help desk services will be delivered from the Supplier's Customer Service Centre (CSC). Access to the Customer Portal (detailed in the General Provisions above) will be made available for call logging by Authorised Users 24/7 or calls can be logged via an email address. For Priority 1 calls only , Authorised Users can contact the help desk via telephone during Core Service Hours:

Dedicated email address:	S4H.helpdesk@nhs.net
Dedicated help desk P1 phone number:	0845 013 0183

All requests for support will be logged on the Supplier's service management system and will be owned by the help desk through to conclusion by the Supplier's support team(s).

Where calls are logged and raised via either the portal or the help desk email, the Supplier's CSC will contact the Authorised User to conduct an initial analysis of the incident / request in order to try and resolve the call. Where it is not possible to resolve the call through the help desk, the Authorised User will be notified and the call will be escalated to the relevant technical support team.

To enable the timely resolution of calls the Buyer will provide:

- A named lead user with current contact details including email and telephone number
- A named IT Department contact with current contact details including email and telephone number
- HSCN / SWAN connection available with up-to-date connection details
- On site access for Supplier staff if required

Service Levels

Response Times

Definition	Service Level
Helpdesk Response Time (measured during Core Service Hours)	All calls raised through the Customer Portal will immediately be given an automatic receipt which will detail the call reference number. Emails will be logged 4 times daily: early morning, mid-morning, early afternoon and mid-afternoon at which point the call reference number will be issued to the Authorised User.

Incident Priority Levels

Incident priority levels are defined as follows:

Priority Level	Definition
Priority 1	Any incident shall be categorised as Priority 1 where an immediate action is required because a significant part of the service is unavailable, resulting in users being unable to perform their duties or a clinical incident arises, in each case which meets the applicable criteria below. A service failure which, in the reasonable opinion of the Buyer and or Authorised User: • constitutes a loss of S4H SaaS which prevents more than 45% of end users or Authorised Users from working; or • has a critical impact on the activities of the Buyer or Authorised User; or • results in any material loss or corruption of Buyer or Authorised User data; or • presents a clinical safety issue; or • prevents an end user or Authorised User from logging an incident with the Help Desk.
Clinical P1	Any untoward or unexpected event which interferes with the treatment of a patient and which results in, or could have resulted in, inappropriate or inadequate clinical care, missed or delays to screening or follow-up services or a breach of confidentiality. Types of activities which could result in a Clinical P1:

Priority Level	Definition
	• loss of record – Authorised User has gone into the system and knows that a record did exist, but it is now missing. (e.g. when screening provider removed in error) • Missing Record – e.g. Birth registered but no record exists in S4H SaaS, incorrect mapping (gone to wrong NHSP site), corrupt data has not reached NHSP Solution , records not coming through from NSS. • Sending of data by insecure means (e-mail, fax etc.) A Clinical P1 will also be a Priority 1 only where the criteria for a Priority 1 have also been met.
Priority 2	A service failure which, in the reasonable opinion of the Buyer and or Authorised User has the potential to: • have a major (but not critical) adverse impact on the activities of the Buyer and or Authorised User; or • cause disruption and or financial loss to the Buyer and or Authorised User which is more than trivial but less severe than the significant disruption described in the definition of a Priority 1 service failure.
Priority 3	A service failure which, in the reasonable opinion of the Buyer and or Authorised User has the potential to have a moderate or minor adverse impact on the activities of the Buyer or Authorised User or which is in respect of guidance and advice. Non exhaustive list of examples: • typically impacts one hospital or Authorised User but could be a minor bug that impacts all users; • a localised printing problem; • local logon issues; • non-clinical display issues; e.g. the data is correct but highlighting of statuses, RAG, rating, etc. may not be functioning.
Priority 4	Bugs and known errors that require patching of the S4H SaaS
Priority 5	Requests for changes to the S4H SaaS where additional functionality or changes to existing functionality are required.

Service Levels for the Core System

The Supplier shall meet or exceed the following Service Levels:

Definition	Measure	Measurement Period
Availability of the Core System	99.7%	Quarterly

Definition	Measure	Measurement Period
Priority 1 incident fix	Resolution within 4 Core Hours	Quarterly
Priority 2 incident fix	Resolution within 1 Business Day	Quarterly
Priority 3 incident fix	85% Resolved within 3 Business Days.	Quarterly
Priority 4 incidents fix (bugs)	75% Resolved within 90 days	
95% Resolved within 180 days	Rolling 90 days	
Rolling 180 days		
Priority 5 incidents (changes)	100% Costed within 90 days	Rolling 90 days
Yearly P1	6 or less a Year	Yearly
Number of technical faults (alerts) reported (e.g. CPU utilisation threshold reached)	In the first Year a month on month reduction of fault reports (alerts)	Yearly
Priority 1 & 2 incidents	In Year Two less than 4 per month	Yearly
Time taken to log on to application (measured from the point at which the user enters the correct password and ending when the initial menu screen appears)	99.9% < 5 seconds	Quarterly

Incident Resolution / Response Times

The Supplier shall record the time at which any incident is logged with the help desk and the time that the incident is subsequently resolved. In the case of incidents reported via the Customer Portal, the user will receive an automated email confirmation with the incident reference number. For the purposes of measuring the applicable Service Level, the point at which the incident is recorded on the call logging system shall be the start time.

The resolution time guidelines which apply to all calls made to the help desk are set out in table above. Measurement of the target times will begin at the earliest point in time during Core Service Hours at which the Incident was registered by the help desk. Timings end (within Core Service Hours) when the Incident has been resolved and resolution notified to the party reporting the incident.

An incident is deemed to be resolved once (i) the cause of the incident has been identified and addressed or (ii) a satisfactory work around has been provided by the Supplier, and at this point the fix time is calculated. An incident can only be closed once the originator has been contacted and has confirmed the incident as being corrected

Both Parties acknowledge and agree that where a satisfactory work around has been provided by the Supplier, the Supplier will, within 60 Core Service Hours of the work around being provided, provide the Buyer with written confirmation as to when a permanent fix will be provided. In any event, the permanent fix must be provided to the

Buyer within a reasonable timeframe (having regard to the nature of the incident and the impact upon the Buyer of complying with the workaround).

Where an incident re-occurs within 24 Core Service Hours of it having been confirmed as corrected, the incident shall be deemed not to have been fixed and the fix time shall be deemed as continuing from the point of the initial call.

Both Parties acknowledge and agree that it may not be possible for all calls to be concluded within proposed guidelines.

From time to time, it may be necessary by mutual agreement to leave an incident open for an extended period in order to monitor for additional occurrences or to evaluate the effect of proposed solutions.

Planned Maintenance

The Supplier shall use reasonable endeavours to provide the Buyer with at least 48 hours advance notice of any planned maintenance of any infrastructure relating to S4H SaaS and to ensure that S4H SaaS is not be unavailable for more than 12 Core Service Hours in any quarter.

Emergency Maintenance

Whenever possible, the Buyer will have at least six hours advance notice of any emergency maintenance of any of the infrastructure relating to S4H SaaS.

Emergency Maintenance of the Supplier's infrastructure will, whenever possible, take place between the hours of 17:30 and 09:00 (UK local time) on a Business Day unless there is an identified and demonstrable immediate risk to the S4H SaaS.

Service Management

The Supplier will appoint a Customer Service Manager (CSM) who will be responsible for ensuring the service is managed and delivered in accordance with the Agreement.

The CSM will provide a single point of contact to the Buyer for all service related aspects of the contract including assistance with reporting, incident escalation and continual service improvement. The CSM will manage processes such as Incident, Problem and Change Management.

A Lead Consultant will also be allocated to work with the Buyer's programme team staff to provide advice, guidance and support in the use of S4H SaaS.

The Supplier shall provide a bi-annual service report to the Buyer, and arrange a follow-up service call to address any issues raised by the Buyer.

Escalation Procedure

The escalation contacts listed below are the relevant people to be contacted once escalation levels have been reached. There are three escalation levels for Priority 1 and Priority 2 levels, with different timescales for each priority escalation level. Each level of escalation is reached if for Priority 1 and 2 issues, an incident is not resolved within the applicable Service Level.

The roles defined are:

The Supplier:

Level 1 – Customer Service Manager

Level 2 - Head of Health Services Delivery

Level 3 - Head of Screening Services

The Buyer:

Level 1 – Screening Local Team Leader

Level 2 – Screening Manager

Level 3 – Head of Audiology

Priority Level	Escalation target time (Hours)	Escalation Level	Supplier Contact	Buyer Contact
1	2	1	Customer Service Manager	Level 1
1	4	2	Customer Service Manager Head of Health Services Delivery	Level 1 Level 2
1	6	3	Customer Service Manager Head of Health Services Delivery Head of Screening Services	Level 1 Level 2 Level 3
2	4	1	Customer Service Manager	Level 1
2	24	2	Customer Service Manager Head of Health Services Delivery	Level 1 Level 2
2	36	3	Customer Service Manager Head of Health Services Delivery Head of Screening Services	Level 1 Level 2 Level 3

Annex: NEC Rego

The additional provisions set out in this Annex apply to the provision of NEC Rego Software as a Service. If there is any conflict between the provisions set out in this Annex and the General Provisions, this Annex shall apply.

Service Overview

Vantage Health provides an advanced digital solution, NEC Rego, to refer patients to the most appropriate providers. The service supports the bidirectional flow of images, clinical data and messages to support electronic referrals, advice and guidance and other clinical communications. Through algorithms, integration with existing clinical and national systems, and intelligent workflow, NEC Rego can be customised to meet local requirements and support all healthcare specialties.

Onboarding Services

Where specified in the Particulars, the following onboarding services are provided:

Project management:

- PRINCE2 project manager working alongside Trust project managers
- Coordination of regular meetings with key stakeholders
- Production and maintenance of project documentation

Customisation:

- Meetings with key stakeholders to map the specialties, reasons for requests and agree Directory of Services (DoS). Confirmation over workflow, provider reporting panel, notifications/alerts and dashboards
- Implementation of algorithms to ensure that the system reflects local requirements
- Change control process to record requested modifications and update the system accordingly

Access and training:

- Liaison with local IT teams to ensure that each practice and provider has access to the system
- Production and delivery of training collateral including user manuals and videos
- Provision of group training sessions

Testing:

- Technical, functional and regression testing
- Smoke testing of the core service elements on a regular basis

Support Services

The Service Desk can be contacted by the Buyer's Authorised Users in the following ways during the following times:

- via the Supplier's customer portal which can be accessed through the URL support.vantage.health ("**Customer Portal**"), 24 hours a day, seven days a week; or
- where the Customer Portal is not available for any reason, through the Service Desk telephone number 0207 993 5870 during Normal Business Hours.

Hosting

The Buyer acknowledges that NEC Rego is hosted in a third party environment provided by Carelink (the trading name for Piksel Limited) using a public cloud solution which, regardless of any other provision in this Agreement, shall be provided in accordance with Carelink's standard terms & conditions to the exclusion of all other terms, including in relation to service availability and support. For clarity, the only Service Levels that shall apply to the Carelink hosting platform component of NEC Rego are those provided by Carelink.

Buyer Obligations:

- Project management of Trust activities
- Appropriate resources available to support the implementation process
- Technical resources available to roll out software required to deliver the solution
- Support of clinical review groups (CRGs) who will review and approve all pathways prior to go-live
- Communications to primary care users
- Ensure availability of appropriate staff for meetings
- Ensure availability of staff for training
- Approval of the NHS Target Operating Model and Clinical Safety Report prior to go-live
- Support with access to practices for implementation, training and ongoing service support

Security, Disaster Recovery and Back-Up Policy

In the section in the General Provisions section of these Supplier Terms headed "*Security, Disaster Recover and Back-Up Policy*", the paragraph beginning "*The Supplier confirms that:*" does not apply and is replaced with the following:

The Supplier confirms that:

- The SaaS is provided via a HSCN cloud for the sole use by or on behalf of the public sector;
- The SaaS hosting platform is underpinned by an ISO 20000 accredited, ITIL managed services, ISO 9001 QMS and ISO 27001 ISMS. The infrastructure is located in a ISO27001 secure facility, independently pen tested and regularly scanned for vulnerabilities;
- It shall comply with the Supplier's Privacy and Security Policy relating to the privacy and security of the Buyer Data;

- The information assurance process as detailed within the paragraphs above will be periodically revised and updated to ensure alignment with good industry practice.

In addition, the following paragraph (again, set out in the General Provisions section of these Supplier Terms under the same heading as above), does not apply: The Buyer recognises that the SaaS is a hosted, multi-tenanted solution. The Buyer Data will be segregated from the data of other Supplier buyers using the SaaS solution and there will be no data sharing facility.

Annex: NEC OptoMize

The additional provisions set out in this Annex apply to the provision of NEC OptoMize Software as a Service. If there is any conflict between the provisions set out in this Annex and the General Provisions, this Annex shall apply.

Hosting

The Buyer acknowledges that NEC OptoMize SaaS is hosted in a third party environment provided by Wemtech using a public cloud solution which, regardless of any other provision in this Agreement, shall be provided in accordance with Wemtech's standard terms & conditions to the exclusion of all other terms, including in relation to service availability and support. For clarity, the only Service Levels that shall apply to the Wemtech hosting platform component of NEC OptoMize are those provided by Wemtech.

Technical Requirements

Service Dependencies

In order to access and use the NEC OptoMize SaaS the Buyer must provide the following:

- An HSCN / Swan Network connection to access NEC OptoMize.
- NEC OptoMize is designed to work over a range of bandwidths, dependent on the number of users, and the type of data to be uploaded / displayed. As a minimum HSCN/ SWAN Network throughput speeds for the Buyer site must be 256kb/s or above.

Backup / Restore

The Supplier will ensure Buyer Data is backed up daily from the live systems using an automated process scheduled to run overnight, taking into account any batch routines and service availability requirements.

The backup tape cycle includes:

- Daily (incremental)
- Weekly (entire image)
- Monthly and annual saves.

Backup tapes are taken off-site daily and stored in a secure location. NEC OptoMize is delivered from two data centres. Each has a physically separate infrastructure, such that a failure in one will not affect another.

Inter-data centre connectivity provides telecommunications resilience and data replication. All production critical data is replicated to the secondary data centre.

The primary data centre has been designed to be highly resilient to meet requirements for performance and availability. All components have in-built redundancy (for example, multiple power supplies, fans, and so on), with components deployed in duplicate in either an active-active or fail-over configuration.

Service Level Agreement

For the purposes of this Service Level Agreement, the following terms shall have the meaning set out below:

Core Service Hours means 8.30am to 5.00pm Monday to Friday excluding bank holidays in England and Wales.

Service Availability

The Supplier provides NEC OptoMize as a fully hosted and supported solution. The Supplier shall use commercially reasonable endeavours to make the service available 24x7x365 subject to downtime for routine and emergency maintenance.

Help Desk

Help desk services will be delivered from the Supplier's Customer Service Centre (CSC). Access to the Customer Portal (detailed in the General Provisions above) will be made available for call logging by Authorised Users 24/7 or calls can be logged via an email address. For Priority 1 calls only, Authorised Users can contact the help desk via telephone during Core Service Hours:

Dedicated email address:	deshelpdesk@necsws.com
Helpdesk Portal:	https://helphub.necsws.com/
Dedicated help desk P1 phone number:	01223 957999

All requests for support will be logged on the Supplier's service management system and will be owned by the help desk through to conclusion by the Supplier's support team(s).

Where calls are logged and raised via either the portal or the help desk email, the Supplier's CSC will contact the Authorised User to conduct an initial analysis of the incident / request in order to try and resolve the call. Where it is not possible to resolve the call through the help desk, the Authorised User will be notified and the call will be escalated to the relevant technical support team.

To enable the timely resolution of calls the Buyer will provide:

- A named lead user with current contact details including email and telephone number
- A named IT Department contact with current contact details including email and telephone number
- HSCN / SWAN connection available with up-to-date connection details
- On site access for Supplier staff if required

Service Levels

Response Times

Definition	Service Level
Helpdesk Response Time (measured during Core Service Hours)	All calls raised through the Customer Portal will immediately be given an automatic receipt which will detail the call reference number. Emails will be logged 4 times daily: early morning, mid-morning, early afternoon and mid-afternoon at which point the call reference number will be issued to the Authorised User.

Incident priority levels are defined as follows:

Priority Level	Definition
Priority 1	Any incident shall be categorised as Priority 1 where an immediate action is required because a significant part of the service is unavailable, resulting in users being unable to perform their duties or a clinical incident arises, in each case which meets the applicable criteria below. A service failure which, in the reasonable opinion of the Buyer and or Authorised User: • constitutes a loss of NEC OptoMize which prevents more than 45% of end users or Authorised Users from working; or • has a critical impact on the activities of the Buyer or Authorised User; or • results in any material loss or corruption of Buyer or Authorised User data; or • presents a clinical safety issue; or • prevents an end user or Authorised User from logging an incident with the Help Desk.
Priority 2	A service failure which, in the reasonable opinion of the Buyer and or Authorised User has the potential to: • have a major (but not critical) adverse impact on the activities of the Buyer and or Authorised User; or • cause disruption and or financial loss to the Buyer and or Authorised User which is more than trivial but less severe than the significant disruption described in the definition of a Priority 1 service failure.
Priority 3	A service failure which, in the reasonable opinion of the Buyer and or Authorised User has the potential to have a moderate or minor adverse impact on the activities of the Buyer or Authorised User or which is in respect of guidance and advice.

Priority Level	Definition
	Non exhaustive list of examples: • typically impacts one hospital or Authorised User but could be a minor bug that impacts all users; • non-clinical display issues; e.g. the data is correct but highlighting of statuses, RAG, rating, etc. may not be functioning.
Priority 4	Bugs and known errors that require patching of NEC OptoMize
Priority 5	Requests for changes to NEC OptoMize where additional functionality or changes to existing functionality are required.

Service Levels for the Core System

The Supplier shall meet or exceed the following Service Levels:

Definition	Measure	Measurement Period
Availability of the Core System	99.7%	Quarterly
Priority 1 incident fix	Resolution within 4 Core Hours	Quarterly
Priority 2 incident fix	Resolution within 1 Business Day	Quarterly
Priority 3 incident fix	85% Resolved within 3 Business Days.	Quarterly
Priority 4 incidents fix (bugs)	75% Resolved within 90 days	
95% Resolved within 180 days	Rolling 90 days	
Rolling 180 days		
Priority 5 incidents (changes)	100% Costed within 90 days	Rolling 90 days
Yearly P1	6 or less a Year	Yearly
Number of technical faults (alerts) reported (e.g. CPU utilisation threshold reached)	In the first Year a month on month reduction of fault reports (alerts)	Yearly
Priority 1 & 2 incidents	In Year Two less than 4 per month	Yearly

Incident Resolution / Response Times

The Supplier shall record the time at which any incident is logged with the help desk and the time that the incident is subsequently resolved. In the case of incidents reported via the Customer Portal, the user will receive an automated email confirmation with the incident reference number. For the purposes of measuring the applicable Service Level, the point at which the incident is recorded on the call logging system shall be the start time.

The resolution time guidelines which apply to all calls made to the help desk are set out in table above. Measurement of the target times will begin at the earliest point in time during Core Service Hours at which the Incident was registered by the help desk. Timings end (within Core Service Hours) when the Incident has been resolved and resolution notified to the party reporting the incident.

An incident is deemed to be resolved once (i) the cause of the incident has been identified and addressed or (ii) a satisfactory work around has been provided by the Supplier, and at this point the fix time is calculated. An incident can only be closed once the originator has been contacted and has confirmed the incident as being corrected

Both Parties acknowledge and agree that where a satisfactory work around has been provided by the Supplier, the Supplier will, within 60 Core Service Hours of the work around being provided, provide the Buyer with written confirmation as to when a permanent fix will be provided. In any event, the permanent fix must be provided to the Buyer within a reasonable timeframe (having regard to the nature of the incident and the impact upon the Buyer of complying with the workaround).

Where an incident re-occurs within 24 Core Service Hours of it having been confirmed as corrected, the incident shall be deemed not to have been fixed and the fix time shall be deemed as continuing from the point of the initial call.

Both Parties acknowledge and agree that it may not be possible for all calls to be concluded within proposed guidelines.

From time to time, it may be necessary by mutual agreement to leave an incident open for an extended period in order to monitor for additional occurrences or to evaluate the effect of proposed solutions.

Planned Maintenance

The Supplier shall use reasonable endeavours to provide the Buyer with at least 48 hours advance notice of any planned maintenance of any infrastructure relating to NEC OptoMize and to ensure that NEC OptoMize is not unavailable for more than 12 Core Service Hours in any quarter.

Emergency Maintenance

Whenever possible, the Buyer will have at least six hours advance notice of any emergency maintenance of any of the infrastructure relating to NEC OptoMize.

Emergency Maintenance of the Supplier's infrastructure will, whenever possible, take place between the hours of 17:30 and 09:00 (UK local time) on a Business Day unless there is an identified and demonstrable immediate risk to the NEC OptoMize.

Service Management

The Supplier will appoint a Customer Service Manager (CSM) who will be responsible for ensuring the service is managed and delivered in accordance with the Agreement.

The CSM will provide a single point of contact to the Buyer for all service related aspects of the contract including assistance with reporting, incident escalation and continual service improvement. The CSM will manage processes such as Incident, Problem and Change Management.

A Consultant will also be allocated to work with the Buyer's programme team staff to provide advice, guidance and support in the use of NEC OptoMize.

The Supplier shall provide a bi-annual service report to the Buyer and arrange a follow-up service call to address any issues raised by the Buyer.

Escalation Procedure

The escalation contacts listed below are the relevant people to be contacted once escalation levels have been reached. There are three escalation levels for Priority 1 and Priority 2 levels, with different timescales for each priority escalation level. Each level of escalation is reached if for Priority 1 and 2 issues, an incident is not resolved within the applicable Service Level.

The roles defined are:

The Supplier:

Level 1 – Customer Service Manager

Level 2 – Product Owner

Level 3 - Head of Health Delivery

The Buyer:

Level 1 – Screening Programme Manager

Level 2 – To be agreed

Level 3 – To be agreed

Priority Level	Escalation target time (Hours)	Escalation Level	Supplier Contact	Buyer Contact
1	2	1	Customer Service Manager	Level 1
1	4	2	Customer Service Manager Product Owner	Level 1 Level 2
1	6	3	Customer Service Manager Product Owner Head of Health Delivery	Level 1 Level 2 Level 3
2	4	1	Customer Service Manager	Level 1
2	24	2	Customer Service Manager Product Owner	Level 1 Level 2
2	36	3	Customer Service Manager Product Owner Head of Health Delivery	Level 1 Level 2 Level 3

Annex: AAA SMaRT SaaS

The additional provisions set out in this Annex apply to the provision of AAA SMaRT SaaS. If there is any conflict between the provisions set out in this Annex and the General Provisions, this Annex shall apply.

These provisions are relevant to all NHS and Approved Screening Service providers of the England, Wales, Scotland and Northern Ireland AAA Screening Programmes. AAA SMaRT SaaS is accessible to all authorised NHS users for the purposes of supporting the UK (Great Britain and Northern Ireland) National AAA Screening Programme. Users need to be connected to the HSCN / SWAN Network.

Technical Requirements

Service Dependencies

In order to access and use the AAA SMaRT SaaS the Buyer must provide the following:

- An HSCN / Swan Network connection to access AAA SMaRT SaaS.
- Bandwidth and Latency Requirements
- AAA SMaRT SaaS is designed to work over a range of bandwidths, dependent on the number of users, and the type of data to be uploaded / displayed. As a minimum HSCN/ SWAN Network throughput speeds for the Buyer site must be 256kb/s or above.

Backup / Restore

The Supplier will ensure Buyer Data is backed up daily from the live systems using an automated process scheduled to run overnight, taking into account any batch routines and service availability requirements.

The backup tape cycle includes:

- Daily (incremental)
- Weekly (entire image)
- Monthly and annual saves.

Backup tapes are taken off-site daily and stored in a secure location. AAA SMaRT SaaS is delivered from two data centres. Each has a physically separate infrastructure, such that a failure in one will not affect another.

Inter-data centre connectivity provides telecommunications resilience and data replication. All production critical data is replicated to the secondary data centre.

The primary data centre has been designed to be highly resilient to meet requirements for performance and availability. All components have in-built redundancy (for example, multiple power supplies, fans, and so on), with components deployed in duplicate in either an active-active or fail-over configuration.

Disaster Recovery

The Supplier confirms that its disaster recovery and business continuity policies, processes and procedures are based on standard BS25999 and ISO 22301:2019.

These support an ITIL IT service continuity management function.

Service Level Agreement

For the purposes of this Service Level Agreement, the following terms shall have the meaning set out below:

Core Service Hours means 9.00am to 5.00pm Monday to Friday excluding bank holidays in England and Wales.

Service Availability

The Supplier provides AAA SMaRT SaaS as a fully hosted and supported solution. The Supplier shall use commercially reasonable endeavours to make the service available 24x7x365 subject to downtime for routine and emergency maintenance.

Help Desk

Help desk services will be delivered from the Supplier's Customer Service Centre (CSC). Access to the Customer Portal (detailed in the General Provisions above) will be made available for call logging by Authorised Users 24/7 or calls can be logged via an email address. For Priority 1 calls only, Authorised Users can contact the help desk via telephone during Core Service Hours:

Dedicated email address:	AAA.helpdesk@nhs.net
Helpdesk Portal:	https://helphub.necsws.com/
Dedicated help desk P1 phone number:	0845 070 5901

All requests for support will be logged on the Supplier's service management system and will be owned by the help desk through to conclusion by the Supplier's support team(s).

Where calls are logged and raised via either the portal or the help desk email, the Supplier's CSC will contact the Authorised User to conduct an initial analysis of the incident / request in order to try and resolve the call. Where it is not possible to resolve the call through the help desk, the Authorised User will be notified, and the call will be escalated to the relevant technical support team.

To enable the timely resolution of calls the Buyer will provide:

- A named lead user with current contact details including email and telephone number
- A named IT Department contact with current contact details including email and telephone number
- HSCN / SWAN connection available with up-to-date connection details
- On site access for Supplier staff if required

Service Levels

Response Times:

Definition	Service Level
Helpdesk Response Time (measured during Core Service Hours)	All calls raised through the Customer Portal will immediately be given an automatic receipt which will detail the call reference number. Emails will be logged 4 times daily: early morning, mid-morning, early afternoon and mid-afternoon at which point the call reference number will be issued to the Authorised User.

Incident priority levels are defined as follows:

Priority Level	Definition
Priority 1	Any incident shall be categorised as Priority 1 where an immediate action is required because a significant part of the service is unavailable, resulting in users being unable to perform their duties or a clinical incident arises, in each case which meets the applicable criteria below. A service failure which, in the reasonable opinion of the Buyer and or Authorised User: • constitutes a loss of the AAA SMaRT SaaS which prevents more than 45% of end users or Authorised Users from working; or • has a critical impact on the activities of the Buyer or Authorised User; or • results in any material loss or corruption of Buyer or Authorised User data; or • presents a clinical safety issue; or • prevents an end user or Authorised User from logging an incident with the Help Desk.
Clinical P1	Any untoward or unexpected event which interferes with the treatment of a patient, and which results in, or could have resulted in, inappropriate or inadequate clinical care, missed or delays to screening or follow-up services or a breach of confidentiality. Types of activities which could result in a Clinical P1: • loss of data (whole records or key parts of records such as demographics or screening activity); • incorrect or missing assignment of record (for example, missing or incorrect screening services attached to record); • corruption, erroneous or deliberate changing of data; • unable to find a record, for instance due to search problems

Priority Level	Definition
	• Unauthorised access or sending of data (e.g. access by unauthorised person, unauthorised exports, letters sent to wrong place, letters sent to parents of deceased baby); • incorrect entering of data (e.g. demographic data , screening results, recall periods etc), that could lead to incorrect pathways being followed • Sending of data by insecure means (e-mail, fax, etc.). A Clinical P1 will also be a Priority 1 only where the criteria for a Priority 1 have also been met.
Priority 2	A service failure which, in the reasonable opinion of the Buyer and or Authorised User has the potential to: • have a major (but not critical) adverse impact on the activities of the Buyer and or Authorised User; or • cause disruption and or financial loss to the Buyer and or Authorised User which is more than trivial but less severe than the significant disruption described in the definition of a Priority 1 service failure.
Priority 3	A service failure which, in the reasonable opinion of the Buyer and or Authorised User has the potential to have a moderate or minor adverse impact on the activities of the Buyer or Authorised User or which is in respect of guidance and advice. Non exhaustive list of examples: • typically impacts one hospital or Authorised User but could be a minor bug that impacts all users; • a localised printing problem; • local logon issues; • non-clinical display issues; e.g. the data is correct but highlighting of statuses, RAG, rating, etc. may not be functioning.
Priority 4	Bugs and known errors that require patching of the AAA SMaRT SaaS
Priority 5	Requests for changes to the AAA SMaRT SaaS where additional functionality or changes to existing functionality are required.

Service Levels for the Core System

The Supplier shall meet or exceed the following Service Levels:

Definition	Measure	Measurement Period
Availability of the Core System	99%	Quarterly

Definition	Measure	Measurement Period
Priority 1 incident fix	Resolution within 4 Core Hours	Quarterly
Priority 2 incident fix	Resolution within 1 Business Day	Quarterly
Priority 3 incident fix	85% Resolved within 3 Business Days.	Quarterly
Priority 4 incidents fix (bugs)	75% Resolved within 90 days	
95% Resolved within 180 days	Rolling 90 days	
Rolling 180 days		
Priority 5 incidents (changes)	100% Costed within 90 days	Rolling 90 days
Yearly P1	6 or less a Year	Yearly
Number of technical faults (alerts) reported (e.g. CPU utilisation threshold reached)	In the first Year a month on month reduction of fault reports (alerts)	Yearly
Priority 1 & 2 incidents	In Year Two less than 4 per month	Yearly
Time taken to log on to application (measured from the point at which the user enters the correct password and ending when the initial menu screen appears)	99.9% < 5 seconds	Quarterly

Incident Resolution / Response Times

The Supplier shall record the time at which any incident is logged with the help desk and the time that the incident is subsequently resolved. In the case of incidents reported via the Customer Portal, the user will receive an automated email confirmation with the incident reference number. For the purposes of measuring the applicable Service Level, the point at which the incident is recorded on the call logging system shall be the start time.

The resolution time guidelines which apply to all calls made to the help desk are set out in table above. Measurement of the target times will begin at the earliest point in time during Core Service Hours at which the Incident was registered by the help desk. Timings end (within Core Service Hours) when the Incident has been resolved and resolution notified to the party reporting the incident.

An incident is deemed to be resolved once (i) the cause of the incident has been identified and addressed or (ii) a satisfactory work around has been provided by the Supplier, and at this point the fix time is calculated. An incident can only be closed once the originator has been contacted and has confirmed the incident as being corrected

Both Parties acknowledge and agree that where a satisfactory work around has been provided by the Supplier, the Supplier will, within 60 Core Service Hours of the work around being provided, provide the Buyer with written confirmation as to when a permanent fix will be provided. In any event, the permanent fix must be provided to the

Buyer within a reasonable timeframe (having regard to the nature of the incident and the impact upon the Buyer of complying with the workaround).

Where an incident re-occurs within 24 Core Service Hours of it having been confirmed as corrected, the incident shall be deemed not to have been fixed and the fix time shall be deemed as continuing from the point of the initial call.

Both Parties acknowledge and agree that it may not be possible for all calls to be concluded within proposed guidelines.

From time to time, it may be necessary by mutual agreement to leave an incident open for an extended period in order to monitor for additional occurrences or to evaluate the effect of proposed solutions.

Planned Maintenance

The Supplier shall use reasonable endeavours to provide the Buyer with at least 48 hours advance notice of any planned maintenance of any infrastructure relating to AAA SMaRT SaaS and to ensure that AAA SMaRT SaaS is not unavailable for more than 12 Core Service Hours in any quarter.

Emergency Maintenance

Whenever possible, the Buyer will have at least six hours advance notice of any emergency maintenance of any of the infrastructure relating to AAA SMaRT SaaS.

Emergency Maintenance of the Supplier's infrastructure will, whenever possible, take place between the hours of 17:30 and 09:00 (UK local time) on a Business Day unless there is an identified and demonstrable immediate risk to the AAA SMaRT SaaS.

Service Management

The Supplier will appoint a Customer Service Manager (CSM) who will be responsible for ensuring the service is managed and delivered in accordance with the Agreement.

The CSM will provide a single point of contact to the Buyer for all service related aspects of the contract including assistance with reporting, incident escalation and continual service improvement. The CSM will manage processes such as Incident, Problem and Change Management.

A Consultant will also be allocated to work with the Buyer's programme team staff to provide advice, guidance and support in the use of AAA SMaRT SaaS.

The Supplier shall provide a bi-annual service report to the Buyer, and arrange a follow-up service call to address any issues raised by the Buyer.

Escalation Procedure

The escalation contacts listed below are the relevant people to be contacted once escalation levels have been reached. There are three escalation levels for Priority 1 and Priority 2 levels, with different timescales for each priority escalation level. Each level of escalation is reached if for Priority 1 and 2 issues, an incident is not resolved within the applicable Service Level.

The roles defined are:

The Supplier:

Level 1 – Customer Service Manager

Level 2 – Product Owner

Level 3 - Head of Health Delivery

The Buyer:

Level 1 – Screening Local Manager

Level 2 – Screening IT Lead

Level 3 – Programme Manager

Priority Level	Escalation target time (Hours)	Escalation Level	Supplier Contact	Buyer Contact
1	2	1	Customer Service Manager	Level 1
1	4	2	Customer Service Manager Product Owner	Level 1 Level 2
1	6	3	Customer Service Manager Product Owner Head of Health Delivery	Level 1 Level 2 Level 3
2	4	1	Customer Service Manager	Level 1
2	24	2	Customer Service Manager Product Owner	Level 1 Level 2
2	36	3	Customer Service Manager Product Owner Head of Health Delivery	Level 1 Level 2 Level 3

Annex: NEC Registries as a Service

Where NEC Registries as a Service is to be provided the provisions set out in this Annex shall apply. If there is any conflict between the provisions set out in this Annex and the General Provisions above, this Annex shall apply.

Use of a third party's public cloud

Where applicable, the Buyer consents to the use of Microsoft Azure as a sub-processor of personal data for the purpose of providing Microsoft Azure cloud services, and acknowledges and agrees to the provision of those services on Microsoft Azure's standard terms.

Glossary

In addition to the terms defined elsewhere in these Supplier Terms (or other parts of the Agreement), the following terms shall have the following meaning:

"Agreement"	means the Call-Off Agreement.
"Authorised Users"	means those employees, agents and independent contractors of the Buyer who are authorised by the Buyer to use the SaaS and the Documentation, as further described in these Supplier Terms.
"Back-Up Policy"	means the specific arrangements for the back-up of Buyer Data as set out in these Supplier Terms, as may be amended from time to time by the Supplier in its sole discretion upon reasonable prior written notice.
"Business Day"	means any day which is not a Saturday, Sunday or bank or public holiday in the UK.
"Buyer's Administrator"	means the person duly appointed by the Buyer to act as its administrator and the Supplier's lead contact for the purposes of the SaaS, as notified by the Buyer to the Supplier.
"Buyer Data"	means the data inputted by the Buyer, or Authorised Users for the purpose of using the SaaS or facilitating the Buyer's use of the SaaS.
"Documentation"	means the written and/or online descriptions of the SaaS features, functions and methods of operation and the instructions provided for its use.
"End User"	means the entity identified as such in the Particulars.
"Normal Business Hours"	means 09:00 to 17:30 UK time, each Business Day.
"Particulars"	means the Order Form.
"Privacy and Security Policy"	means the Supplier's policy relating to the privacy and security of the Buyer Data, as may be amended from time to time by the Supplier in its sole discretion, which is available on request.
"SaaS"	means the Software as a Service to be delivered as set out in the Particulars.
"SaaS Term"	means the term specified in the Particulars.
"SaaS Portal"	has the meaning set out in these Supplier Terms.
"Service Desk"	means the Supplier's service desk, as described in these Supplier Terms.
"Virus"	means any thing or device (including any software, code, file or program) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any program or data, including the reliability of any program or data (whether by re-arranging, altering or erasing the program or data in whole or part or

otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.