

Order Form

Framework agreement reference: SBS/19/AB/WAB/9411

Date of order	TBA	Order Number	W75114 To be quoted on all correspondence relating to this Order
----------------------	------------	---------------------	---

FROM

Customer	NHS Business Services Authority (" Customer ")
Customer's Address	Stella House, Goldcrest Way, Newburn Riverside Business Park, Newcastle upon Tyne, NE15 8NY
Invoice Address	As above
Contact Ref:	Name: [REDACTED] Address: Stella House, Goldcrest Way, Newburn Riverside Business Park, Newcastle upon Tyne, NE15 8NY e-mail: [REDACTED]

TO

Supplier	Phoenix Software Limited (" Supplier ")
Supplier's Address	Bytes House, Randalls Way, Leatherhead, Surrey, United Kingdom, KT22 7TW
Account Manager	Name: [REDACTED] Address: Bytes House, Randalls Way, Leatherhead, Surrey, United Kingdom, KT22 7TW Phone: [REDACTED] e-mail: [REDACTED]

GUARANTEE

Guarantee to be provided	No
--------------------------	-----------

Where a guarantee is to be provided then this Contract is conditional upon the provision of a Guarantee to the Customer from the Guarantor in respect of the Supplier. Details of the Guarantor (if any) are set out below:

[Parent Company]	Not Required
Parent Company address	
Account Manager	

1. TERM
(1.1) Commencement Date

01 April 2024
(1.2) Expiry Date 31/03/2027 The contract will include one optional 12-month extension period to be activated no less than 30 days before the current Expiry Date.

2. GOODS AND SERVICES REQUIREMENTS	
(2.1) Goods and/or Services	
Goods – 1 X Vantage Software Annual Licence The Customer agrees to purchase all of its requirements for the Goods or equivalent goods from the Supplier.	
Minimum Order Value	£20,516.08 (Exc. VAT)
Total Order Value (Inc. Optional Extension)	£27,629.80 (Exc. VAT)
(2.2) Premises	
Stella House, Goldcrest Way, Newburn Riverside Business Park, Newcastle upon Tyne, NE15 8NY	
(2.3) Lease/ Licenses	
N/A	
(2.4) Standards	
The standards required for this Call-Off Contract are as follows: As per the Supplier's solution	
(2.5) Security Requirements	
Security Policy	
Detailed in Appendix A of this Order Form	
Processing personal data under or in connection with this contract	
YES – Names, contact information, type of injury, crime or allegation of a crime.	
(2.6) Exit Plan (where required)	

NO
(2.7) Environmental Plan
NO
Environmental Policy
Detailed in Appendix B of this Order Form

3. SUPPLIER SOLUTION
(3.1) Supplier Solution
Detailed in Appendix C of this Order Form
(3.2) Account structure including Key Personnel
<div>████████████████████ Sales Executive - Public Sector - Healthcare at Phoenix Software Limited ("Supplier")</div> <div>████████████████████ Chief Executive at Vantage Technologies ("Vendor")</div>
(3.3) Sub-contractors to be involved in the provision of the Services and/or Goods
N/A
(3.4) Outline Security Management Plan
N/A
(3.5) Relevant Convictions
N/A
(3.6) Implementation Plan
The Vantage Software Annual Licence is already installed at the NHSBSA.

4. PERFORMANCE QUALITY
(4.1) Key Performance Indicators
N/A
(4.2) Service Levels and Service Credits
When providing the Goods and/or Services, the Supplier shall as a minimum ensure that it achieves the following service levels:

If the level of performance of the Supplier during the Contract Period:

- (i) fails to achieve a Service Level in respect of each element of the Service, then the Customer shall be entitled to deduct the Service Credits from the Contract Price; and/or
- (ii) constitutes a Critical Service Failure, the Customer shall be entitled to terminate this Contract.

5. PRICE AND PAYMENT

(5.1) Contract Price payable by the Customer in accordance with the commercial schedule set out in the framework agreement (including applicable discount but excluding VAT), payment profile and method of payment (e.g. Government Procurement Card (GPC) or BACS))

Initial contract value: £20,516.08 ex. VAT

Total contract value (including Year 4): £27,629.80 ex. VAT

Payment to be made via BACS

(5.2) Invoicing and Payment

The Supplier shall issue invoices annually in arrears. The Customer shall pay the Supplier within 30 days of receipt of a valid Invoice, submitted in accordance with this paragraph 5.2, the payment profile set out in paragraph 5.1 above and the provisions of the Contract.

Specific arrangements relating to the above payment method are:

- Via email (preferred) to: [REDACTED]
- Or by post to: Stella House, Goldcrest Way, Newburn Riverside Park, Newcastle-Upon Tyne, Tyne & Wear, NE15 8NY

6. SUPPLEMENTAL AND/OR ADDITIONAL CLAUSES

(6.1) Supplemental requirements

Not used

BY SIGNING AND RETURNING THIS ORDER FORM THE SUPPLIER AGREES to enter a legally binding contract with the Customer to provide the Goods and/or Services. The Parties hereby acknowledge and agree that they have read the NHS Conditions of Contract for purchase of goods and/or Services and by signing below agree to be bound by the terms of this Contract.

Principal Signatory Details

For the Buyer:

Title: Senior Commercial Officer

Name: [REDACTED]

Email: [REDACTED]

For the Supplier:

Title: Healthcare Team Manager

Name: [REDACTED]

Email: [REDACTED]

Signed	For and on behalf of the Supplier	For and on behalf of the Buyer
	Signed via DocuSign on 19/02/2024	Signed via DocuSign on 20/02/2024

Appendix A: Buyer's Security Policy

Information Security Policy

Issue sheet

Document reference	ISMSPOL 001
Document location	ISMS>Document control>Document review 2023
Title	NHSBSA Information Security Policy
Author	Information Security & Business Continuity Manager
Owner	NHSBSA CEO and NHSBSA SIRO
Issued to	All NHSBSA staff
Reason issued	For information/action
Last reviewed	March 2023
Review Cycle	Two years
Date of Wellbeing and Inclusion Assessment	No Impact
Date of Fraud Review	No Impact

Revision details

Version	Date	Amended by	Approved by	Details of amendments
V1.0	February 2019	Lead Information Security Risk Manager	BISG	Info sec policy statement signed and ISMSPOL 001 communicated to staff
V2.0	February 2020	Information Security Risk and BC Manager	BISG	Approved at BISG 20/02/2020 – communicated to all staff.
V3.0	January 2021	Information Security Risk and BC Manager	BISG	Approved at BISG
V4.0	March 2023	Information Security & Business Continuity Manager	BISG	Full review to reflect revised structure.

Information security policy statement

The NHSBSA is committed to ensuring that we manage our information, and the information of our clients and stakeholders that we manage on their behalf, securely. This means that we will implement, and monitor the effectiveness of, controls designed to preserve its confidentiality, integrity, and availability in line with our business and legal and regulatory requirements.

Our information security objectives are aligned to our business objectives and are delivered through our information security management system (ISMS).

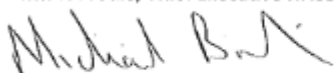
Our ISMS is certified to the *ISO27001:2013 Information security management system* standard to ensure that it is independently and regularly assessed for effectiveness and continual improvement.

We have established an information security governance framework and allocated specific roles, responsibilities, and resources to ensure that our ISMS is

- implemented effectively,
- responsive to changes in legal and regulatory requirements,
- responsive to changes to the threat landscape

In support of our specific roles and responsibilities we have an ongoing information security training and awareness programme to ensure that all NHSBSA staff, contractors, and suppliers understand their responsibilities for handling information securely.

Michael Brodie, Chief Executive NHSBSA



Mark Dibble, SIRO NHSBSA



1. Purpose

- 1.1. This policy is our 'Statement of Management Intent' and is supported by topic-specific policies, each of which will be delivered through appropriate information security standards, processes, procedures and guidelines.
- 1.2. This policy is intended to be read and understood by all NHSBSA staff and stakeholders responsible for managing, maintaining, delivering and assessing the effectiveness of our information security management programme.

2. Governance, Roles, and Responsibilities

- 2.1 There is an established information security management governance structure in place which is shown in Annex 1.
- 2.2 Key roles and responsibilities are given below.

Accounting Officer

Our Accounting Officer is the Chief Executive who has overall organisational accountability for effective information security management across the NHSBSA.

Senior Information Risk Owner (SIRO)

Our SIRO is responsible for taking ownership of our information risk policy, acting as an advocate for information risk to the Board, and providing advice to the Accounting Officer on the content of governance statements regarding information risk.

Caldicott Guardian

Our Caldicott Guardian is responsible for ensuring the confidential information of our service users is used ethically, legally and appropriately.

Data Protection Officer

Our Data Protection Officer is responsible for informing and advising NHSBSA employees and stakeholders of their data protection obligations and collaborating with them on managing the relevant privacy risks for customers and staff.

Information Asset Owner (IAO)

Information Asset Owners are Directors of NHSBSA responsible for

- understanding and addressing risks to the information asset they 'own'

- providing assurance to the SIRO on the security and use of their assets, and the effective management of information risk
- maintaining the confidentiality of their information assets, ensuring that access to assets is controlled and that the information is securely kept
- ensuring personal data is identified, securely handled and can be used in ways that it is needed
- ensuring information is appropriately protected and proper safeguards are applied when it is shared
- ensuring information is managed appropriately during and following change
- maintaining an understanding of 'owned' assets and how they are used
- knowing what information is held and who has access to it for what purpose
- leading and fostering a culture that values, protects and uses information for the public good

Information Asset Administrator (IAA)

Information Asset Administrators are Heads of Service of NHSBSA responsible for

- providing day-to-day support to the IAO in managing information risks in their area
- ensuring that information security and governance policies and procedures are followed
- ensuring their information asset registers are accurate and up to date
- approving service-based information security risk assessments and risk treatment plans
- ensuring compliance with data sharing agreements within their service
- ensuring service-based information handling procedures are fit for purpose and properly applied
- recognising new information handling requirements and consulting with their IAO over appropriate procedures
- ensuring appropriate access to their information is monitored and maintained

Head of Security & Information Governance

Our Head of Security & Information Governance is responsible for

- monitoring the effectiveness of our information security management programme
- providing expert advice to the business on all information security management matters
- ensuring that information security risks are assessed in a timely manner and treated in accordance with our approved risk appetite

Information Security & Business Continuity Manager

Our Information Security & Business Continuity Manager is responsible for managing the implementation, effective delivery and continual improvement of our

- information security management system
- information security assurance programme
- information security compliance framework
- business continuity management programme

Head of Cyber Security and Infrastructure Services

Our Head of Cyber Security and Infrastructure Services is responsible for

- providing expert advice to the business on all matters concerning technical security
- ensuring the operational effectiveness of technical security controls and processes
- being accountable for technical information security regulatory compliance across the NHSBSA

Cyber Security Operations Manager

Our Cyber Security Operations Manager is responsible for

- providing advice and guidance around cyber security threats and vulnerabilities
- providing cyber security architecture and engineering resource to facilitate safe design and implementation of products and technical security controls
- ensuring that all technical security risks are appropriately managed
- monitoring technical security systems and controls and effectively managing alerts
- timely reporting and investigation of cyber security incidents

Staff and contractors

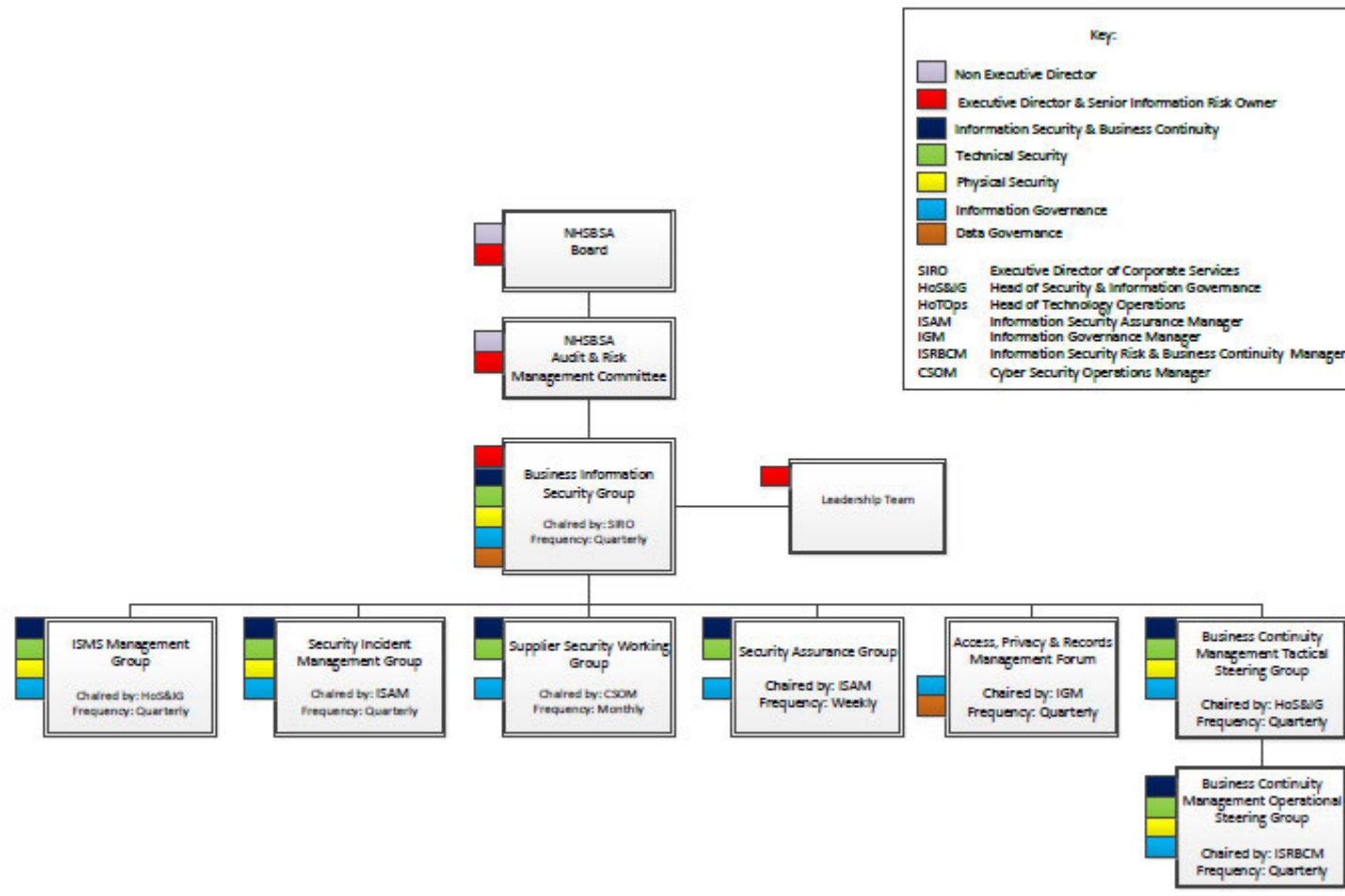
NHSBSA staff and contractors are responsible for

- complying with NHSBSA information security policies, standards, processes and procedures and the appropriate protection of information assets
- being accountable for their actions in relation to the security of information that they manage, process or control
- completing annual training in a timely manner to ensure that information security roles and responsibilities are understood
- safeguarding hardware, software and information in their care

3. Compliance

- 3.1 In applying this policy, the NHSBSA will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.
- 3.2 Compliance with this policy **is** subject to internal and external audit to ensure its effectiveness.

Annex 1 – ISMS Governance Structure



Appendix B: Buyer's Environmental Policy

Environmental policy

The NHSBSA is a Special Health Authority and an Arm's Length Body (ALB) of the Department of Health (DH). We provide a range of critical central services to NHS organisations, NHS contractors, patients and the public. The NHSBSA was created in 2006 by bringing together a number of previously separate NHS organisations. We still deliver the core range of services we started with and have taken on additional services as our stakeholders' needs have evolved.

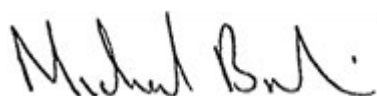
We recognise that our activities, products and services, and the way we choose to deliver them, can have both a negative and positive impact upon the environment, and therefore an impact upon our employees and local communities.

We are committed to:

- ✓ becoming a Net Zero organization by 2030
- ✓ protecting the environment and preventing pollution caused by what we do
- ✓ ensuring that we comply with environmental laws related to what we do, and meeting the requirements of other policies, strategies etc. we support such as those created by Government, Department of Health and NHS
- ✓ continually improve our environmental management system to enhance our performance by setting and reviewing objectives and targets relevant to the NHSBSA each year. We focus on:
 - maintaining an appropriate governance framework, which ensures continual improvement and a commitment to fulfil our compliance obligations
 - reducing greenhouse gas emissions and adapting to climate change
 - reducing waste and maximising resource efficiency
 - reducing water use
 - creating wider environmental, social and economic value, through our activities and our supply chain

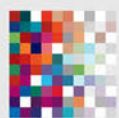
We will achieve this by:

- ✓ operating an NHSBSA-wide environmental management system, which instructs staff and others on how to carry out key activities
- ✓ training and coaching staff (and others where appropriate) to ensure they understand how to play their part
- ✓ communicating with staff (and others where appropriate) about environmental issues
- ✓ actively engaging with relevant forums and groups to learn from others and share our knowledge and experience



Michael Brodie, Chief Executive NHSBSA

Appendix C: Supplier's Solution



VANTAGE
TECHNOLOGIES



One Licence.

One Platform. Multiple Solutions.

Vantage Technologies was established in 1988 and quickly grew to be a major provider of data management solutions in the UK. In August 2016, working from our head office in Sheffield, Vantage launched a variety of data management solutions that can be easily configured for every organisation's unique requirements. Vantage now has over 30 years experience in developing fit for purpose data management solutions to a variety of organisations in multiple sectors and continue to proudly deliver excellent savings, efficiencies and fanatical support.

Our Enterprise Software

Our **Enterprise Software** offers multiple data management solutions integrated into one system that can effectively be used by any organisation or company looking to streamline their data input and retrieval procedures. Our Enterprise Software can be used to send and receive data from other systems for comprehensive data sharing and fast and efficient implementation.



**Multi Device
Compatible**



**Web-based Software
For Access Anywhere**



**ISO 27001
Certified**



**Comprehensive
Reporting**

Software Modules

Our **Enterprise Software** offers a substantial catalogue of database templates that are ready to use and are easily customisable in order to fit your organisation's specific needs. Each of our modules are designed to work seamlessly together, creating easily searchable links between relevant datasets.

With our **Enterprise Software** your organisation will be able to efficiently manage numerous organisational procedures and processes using the below software modules.



Database Template Library

Compliance, Audit, Performance and Quality Management

**Audit &
Quality
Management**

**Performance
Management**

**Complaints
Management**

**Help Desk
Management**

**Central Alerts
System**

**Compliance &
Standards
Management**

**Policy
Management**

**Contract
Management**

**Freedom to
Speak Up**

**Service User
Records**

**Occupational
Health
Referrals**

**Supervision
Management**

**Subject
Access
Requests**

**GDPR
Management**

**Training
Management**

**Practices &
Privileges**

Risk, Safety and Incident Management

**Incident
Management**

**Health &
Safety**

**Risk
Management**

**Risk
Assesment**

Business, Facility and Asset Management

**Faciltiy &
Asset
Management**

**Volunteer
Management**

**Contractor
Management**

**Vehicle &
Machine
Management**

**Customer
Relationship
Management**

**Donation &
Finance
Management**

**File Store
Management**

**Event
Management**

**Human
Resources
Management**

**Portable
Appliance
Testing**

**Planned
Preventative
Maintenance**

**Surveys &
Feedback
Management**

How we Help Charities & Healthcare Organisations

We work with charities and healthcare organisations to develop fit for purpose software solutions that fit with each organisations unique requirements.

Each of our software modules are designed to work seamlessly together to save your organisation valuable time and resources.

Whether you are looking to employ a more effective database management system, perform audits and inspections more efficiently, or improve responses to incidents and complaints, Vantage Technologies can supply you with a highly adaptable and secure system tailored to your needs.

One Licence

Our Annual Software Licence

Our **One Licence** offers excellent value for money allowing you access to our full catalogue of data management solutions and database templates, pairing our One Licence with our Enterprise Software provides you with the ultimate flexibility to implement the solutions your organisation requires. Our One Licence operates as a software as a service (SaaS) licence, allowing your organisation access to our Enterprise Software as an annual subscription.

What are the benefits?

- ✓ **Unlimited Solutions & Database Templates**
- ✓ **Unlimited Amount of System Users**
- ✓ **Access to Bespoke and Custom Solutions**
- ✓ **Excellent Savings & Efficiencies**



Why Vantage?

Why choose Vantage as your data management software provider?

- ✓ Over 30 Years of Industry Experience
- ✓ Continuous Help & Support
- ✓ ISO 27001 Certified
- ✓ Excellent Savings & Efficiencies
- ✓ Continuous Software Development



Our Mission

"We thrive on the fanatical support we offer to our customers in order to streamline and enhance their organisation's data management procedures and processes. We aim to continue delivering exceptional customer support to align with our comprehensive, affordable and efficient data management software."

Book a **FREE** Software Demonstration

Get in touch to book a free software demonstration and start your Vantage journey today!

demo@vantage-technologies.co.uk



0114 247 9500



www.vantage-technologies.co.uk

Appendix D: Supplier's Terms and Conditions

Ref: xxx

Vantage Technologies Limited

Software as a Service Agreement

In respect of the

***Vantage Hosted Managed
Service***





Date: 2024

PARTIES

1. **Vantage Technologies Limited**, a company incorporated in England and Wales (registration number 03078362) having its registered office at Vantage House, Rother Valley Way, Sheffield, S20 3RW (the "Provider"); and
2. **XXXXXXXXXXXXXXXXXXXX**, a company incorporated in England and Wales (registration number xxxxxxxx) having its registered office at xxxxxx, xxxxxxxxxxxxxxxxxxxx, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx(the "Customer").

AGREEMENT

1. Definitions

- 1.1 In this Agreement, except to the extent expressly provided otherwise:

"Account" means an account enabling a person to access and use the Hosted Services, including both administrator accounts and user accounts;

"Agreement" means this agreement including any Schedules, and any amendments to this Agreement from time to time;

"Business Day" means any weekday other than a bank or public holiday in England;

"Business Hours" means the hours of 09:00 to 17:00 on a Business Day;

"Charges" means the following amounts:

- (a) the amounts specified in Part 2 of Schedule 1 (Hosted Services particulars);
- (b) such amounts as may be agreed in writing by the parties from time to time.

"Customer Confidential Information" means:

- (a) any information disclosed by or on behalf of the Customer to the Provider at any time before the termination of this Agreement (whether disclosed in writing, orally or otherwise) that at the time of disclosure:
 - () was marked as "confidential"; or
 - () should have been reasonably understood by the Provider to be confidential; and
- (b) the Customer Data; and
- (c) the Customer Personal Data.



"Customer Data" means all data, works and materials: uploaded to or stored on the Platform by the Customer; transmitted by the Platform at the instigation of the Customer; supplied by the Customer to the Provider for uploading to, transmission by or storage on the Platform; or generated by the Platform as a result of the use of the Hosted Services by the Customer (but excluding analytics data relating to the use of the Platform and server log files);

"Customer Personal Data" means any Personal Data that is processed by the Provider on behalf of the Customer in relation to this Agreement;

"Data Protection Laws" means all applicable laws relating to the processing of Personal Data and privacy from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder (DPA 2018)); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended;

"Documentation" means the documentation for the Hosted Services produced by the Provider and delivered or made available by the Provider to the Customer;

"Effective Date" means the date shown at the top of this Agreement even if the Agreement is executed after this date;

"Force Majeure Event" means an event, or a series of related events, that is outside the reasonable control of the party affected (including failures of the internet or any public telecommunications network, hacker attacks, denial of service attacks, virus or other malicious software attacks or infections, or power failures, (in each case, not personal to the particular affected party), industrial disputes, changes to the law, disasters, explosions, fires, floods, riots, terrorist attacks and wars);

"Good Industry Practice" means the exercise of that degree of skill, care, and prudence, as would be expected from a reasonably skilled and experienced company within the same or similar industry, or business sector;

"Hosted Services" means Vantage Enterprise Hosted Service which will be made available by the Provider to the Customer as a service via the internet in accordance with this Agreement;

"Hosted Services Defect" means a defect, error or bug in the Platform having a material adverse effect on the appearance, operation, functionality or performance of the Hosted Services, but excluding any defect, error or bug caused by or arising directly as a result of:

- (a) any act or omission of the Customer or any person authorised by the Customer to use the Platform or Hosted Services;
- (b) any use of the Platform or Hosted Services contrary to the



Documentation, whether by the Customer or by any person authorised by the Customer;

- (c) a failure of the Customer to perform or observe any of its obligations in this Agreement; and/or
- (d) an incompatibility between the Platform or Hosted Services and any other system, network, application, program, hardware or software not specified as compatible in the Hosted Services Specification;

"Hosted Services Specification" means the specification for the Platform and Hosted Services set out in Part 1 of Schedule 1 (Hosted Services particulars) and in the Documentation;

"Intellectual Property Rights" means all intellectual property rights wherever in the world, whether registrable or unregistrable, registered or unregistered, including any application or right of application for such rights (and these "intellectual property rights" include copyright and related rights, database rights, confidential information, trade secrets, know-how, business names, trade names, trademarks, service marks, passing off rights, unfair competition rights, patents, petty patents, utility models, semi-conductor topography rights and rights in designs);

"Maintenance Services" means the general maintenance of the Platform and Hosted Services, and the application of Updates and Upgrades;

"Personal Data" has the meaning given to it in the Data Protection Law;

"Platform" means the data management tools, including the application and database software for the Hosted Services, the system and server software used to provide the Hosted Services, and the computer hardware on which that application, database, system and server software is installed;

"Schedule" means any schedule attached to the main body of this Agreement;

"Services" means any services that the Provider provides to the Customer, or has an obligation to provide to the Customer, under this Agreement;

"Service Level Agreement" means the response and resolution times for the provision of Support Services set out in Part 4 of Schedule 1 (Hosted Services particulars);

"Site" means both a test and live Customer instance of the Hosted Services;

"Support Services" means support in relation to the use of, and the identification and resolution of errors in, the Hosted Services, but shall not include the provision of training services;



"Supported Web Browser" means the most recent version of Microsoft Edge, Mozilla Firefox, Google Chrome or other W3C standard compliant browser. Please note that Microsoft Internet Explorer is explicitly not supported;

"Term" means the term of this Agreement, commencing in accordance with Clause 3.1 and ending in accordance with Clause 3.2;

"UK GDPR" has the meaning given to it in Section 3(10) (as supplemented by section 205(4) of the DPA 2018;

"Update" means a hotfix, patch or minor version update to any Platform software;

"Upgrade" means a major version upgrade of any Platform software; and

"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 compute 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

3. Term

3.1 This Agreement shall come into force upon the Effective Date.

3.2 This Agreement shall continue in force indefinitely subject to termination in accordance with Clause 18 or any other provision of this Agreement.

4. Hosted Services

4.1 The Provider shall create a Site for the Customer and shall provide to the Customer login details for that Site on or promptly following the Effective Date.

4.2 The Provider hereby grants to the Customer a worldwide, non-exclusive licence to use the Hosted Services by means of a Supported Web Browser for the internal business purposes of the Customer in accordance with the Documentation during the Term.

4.3 The Hosted Services may only be used by the officers, employees, agents and subcontractors of the Customer.

4.4 Except to the extent expressly permitted in this Agreement or required by law on a non-excludable basis, the licence granted by the Provider to the Customer



under Clause 4.2 is subject to the following prohibitions:

- (a) the Customer must not sub-license its right to access and use the Hosted Services;
- (b) the Customer must not permit any unauthorised person to access or use the Hosted Services;
- (c) the Customer must not use the Hosted Services to provide services to third parties;
- (d) the Customer must not republish or redistribute any content or material from the Hosted Services save as to customise the Documentation for their own internal purposes;
- (e) the Customer must not make any alteration to the Platform except those allowed by the platform management tools; and
- (f) the Customer must not conduct or request that any other person conduct any load testing or penetration testing on the Platform or Hosted Services without the prior written consent of the Provider.

4.5 The Customer shall use reasonable endeavours, including reasonable security measures relating to administrator Account access details, to ensure that no unauthorised person may gain access to the Hosted Services using an administrator Account.

4.6 The Provider undertakes that the Hosted Services will be performed in accordance with the Documentation and with reasonable skill and care and in accordance with Good Industry Practice. The Provider shall use all reasonable endeavours to maintain the availability of the Hosted Services to the Customer but does not guarantee 100% availability.

4.7 For the avoidance of doubt, downtime caused directly by any of the following shall not be considered a breach of this Agreement:

- (a) a Force Majeure Event;
- (b) a fault or failure of the internet or any public telecommunications network;
- (c) a fault or failure of the Customer's computer systems or networks;
- (d) any breach by the Customer of this Agreement; or
- (e) scheduled maintenance carried out in accordance with this Agreement.

4.8 The Customer must comply with Schedule 2 (Acceptable Use Policy) and must ensure that all persons using the Hosted Services with the authority of the Customer



or by means of an administrator Account comply with Schedule 2 (Acceptable Use Policy).

- 4.9 The Customer must not use the Hosted Services in any way that causes, or may cause, damage to the Hosted Services or Platform or impairment of the availability or accessibility of the Hosted Services.
- 4.10 The Customer must not use the Hosted Services:
- (a) in any way that is unlawful, illegal, fraudulent, or harmful; or
 - (b) in connection with any unlawful, illegal, fraudulent, or harmful purpose or activity.
- 4.11 For the avoidance of doubt, the Customer has no right to access the software code (including object code, intermediate code, and source code) of the Platform, either during or after the Term.
- 4.12 The Provider may suspend the provision of the Hosted Services if any amount due to be paid by the Customer to the Provider under this Agreement is overdue, and the Provider has given to the Customer at least 30 days' written notice, following the amount becoming overdue, of its intention to suspend the Hosted Services on this basis. For the avoidance of doubt, if the Customer makes payment within the 30 days' notice period, the Hosted Services shall not be suspended.

5. Maintenance Services

- 5.1 The Provider shall provide the Maintenance Services to the Customer during the Term.
- 5.2 The Provider shall where practicable give to the Customer at least **5** Business Days' prior written notice of scheduled Maintenance Services that are likely to affect the availability of the Hosted Services or are likely to have a material negative impact upon the Hosted Services, without prejudice to the Provider's other notice obligations under this main body of this Agreement.
- 5.3 The Provider shall give the Customer at least **10** Business Days' prior written notice of the application of an Upgrade to the Platform and shall liaise with the Customer in regard to such Upgrade being applied.
- 5.4 The Provider shall give the Customer at least **2** Business Days' prior written notice of the application of any Update to the Platform and shall liaise with the Customer in regards to such Update being applied. Notwithstanding the foregoing, if the Provider requires to apply a necessary and urgent Update, the Provider shall provide the Customer with as much written of such Update being made as is reasonably



practicable.

- 5.5 The Provider shall provide the Maintenance Services with reasonable skill and care and in accordance with Good Industry Practice.
- 5.6 The Provider may suspend the provision of the Maintenance Services if any amount due to be paid by the Customer to the Provider under this Agreement is overdue, and the Provider has given to the Customer at least 30 days' written notice, following the amount becoming overdue, of its intention to suspend the Maintenance Services on this basis.

6. Support Services

- 6.1 The Provider shall provide the Support Services to the Customer during the Term.
- 6.2 The Provider shall make available to the Customer a helpdesk in accordance with the provisions of this main body of this Agreement.
- 6.3 The Provider shall provide the Support Services with reasonable skill and care and in accordance with Good Industry Practice.
- 6.4 The Provider shall respond to all requests for Support Services made by the Customer through the helpdesk in accordance with the Service Level Agreement.
- 6.5 The Provider may suspend the provision of the Support Services if any amount due to be paid by the Customer to the Provider under this Agreement is overdue, and the Provider has given to the Customer at least **30** days' written notice, following the amount becoming overdue, of its intention to suspend the Support Services on this basis. For the avoidance of doubt, if the Customer makes payment within the **30** days' notice period, the Hosted Services shall not be suspended.

7. Customer Data

- 7.1 The Customer hereby grants to the Provider a non-exclusive, non-transferable licence to use the Customer Data to the extent necessary for the performance of the Provider's obligations and the exercise of the Provider's rights under this Agreement.
- 7.2 The Customer will take reasonable steps to ensure that, to the best of their knowledge, the Customer Data when used by the Provider in accordance with this Agreement will not infringe the Intellectual Property Rights or other legal rights of any person, and will not breach the provisions of any law, statute or regulation, in any jurisdiction and under any applicable law.



7.3 The Provider shall create a back-up copy of the Customer Data at least daily, shall ensure that each such copy is sufficient to enable the Provider to restore the Hosted Services to the state they were in at the time the back-up was taken, and shall retain and securely store such copy onsite at the data center for a period of 14 days.

7.4 Within the period of 1 Business Day following receipt of a written request from the Customer, the Provider shall use all reasonable endeavours to restore to the Platform the Customer Data stored in any back-up copy created and stored by the Provider in accordance with Clause 7.3. The Customer acknowledges that this process will overwrite the Customer Data stored on the Platform prior to the restoration.

8. No assignment of Intellectual Property Rights

8.1 Nothing in this Agreement shall operate to assign or transfer any Intellectual Property Rights from the Provider to the Customer, or from the Customer to the Provider.

9. Charges

9.1 The Customer shall pay the Charges to the Provider in accordance with this Agreement.

9.2 The Charges are for a full twelve months and early termination in accordance with clause 18 does not entitle the Customer to a refund, or credit, for any unused time, unless the Customer terminates the Agreement early because of a material breach of any term of this Agreement by the Provider, or if the Provider terminates the Agreement early on the basis of convenience (in accordance with Clause 18.1), in which case the Customer shall be entitled to such refund for any unused time.

9.3 All amounts stated in or in relation to this Agreement are, unless the context requires otherwise, stated exclusive of any applicable value added taxes, which will be added to those amounts and payable by the Customer to the Provider.

9.4 The Provider may elect to vary any element of the Charges on any anniversary of the Effective Date of this Agreement, providing that no such variation shall result in an aggregate percentage increase in the relevant element of the Charges during the Term that exceeds the percentage increase, during the same period, in the Retail Prices Index (all items) published by the UK Office for National Statistics.



10. Payments

- 10.1 The Provider shall issue invoices for the Charges to the Customer on or after the invoicing dates set out in Part 2 of Schedule 1 (Hosted Services particulars).
- 10.2 The Customer must pay the Charges to the Provider within the period of 30 days following the issue of an invoice in accordance with this Clause 10 providing that the Charges must in all cases be paid before the commencement of the period to which they relate.
- 10.3 The Customer must pay the Charges by bank transfer or cheque (using such payment details as are notified by the Provider to the Customer from time to time).
- 10.4 If the Customer does not pay any amount properly due to the Provider under this Agreement, the Provider may charge the Customer interest on the overdue amount at the rate of 4% per year above the base rate of Royal Bank of Scotland Plc from time to time.

11. Provider's confidentiality obligations

- 11.1 The Provider must:
 - (a) keep the Customer Confidential Information strictly confidential;
 - (b) not disclose the Customer Confidential Information to any person without the Customer's prior written consent, and then only under conditions of confidentiality approved in writing by the Customer.
 - (c) use the same degree of care to protect the confidentiality of the Customer Confidential Information as the Provider uses to protect the Provider's own confidential information of a similar nature, being at least a reasonable degree of care;
 - (d) act in good faith at all times in relation to the Customer Confidential Information; and
 - (e) not use any of the Customer Confidential Information for any purpose other than performing the Services under this Agreement.

Notwithstanding Clause 11.1, the Provider may disclose the Customer Confidential Information to the Provider's officers, employees, professional advisers, insurers, agents, and subcontractors who have a need to access the Customer Confidential Information for the performance of their work with respect to this Agreement and who are bound by a written agreement or professional obligation to protect the confidentiality of the Customer Confidential Information.



- 11.2 This Clause 11 imposes no obligations upon the Provider with respect to Customer Confidential Information that:
- (a) is known to the Provider before disclosure under this Agreement and is not subject to any other obligation of confidentiality;
 - (b) is or becomes publicly known through no act or default of the Provider; or
 - (c) is obtained by the Provider from a third party in circumstances where the Provider has no reason to believe that there has been a breach of an obligation of confidentiality.
- 11.3 The restrictions in this Clause 11 do not apply to the extent that any Customer Confidential Information is required to be disclosed by any law or regulation, by any judicial or governmental order or request, or pursuant to disclosure requirements relating to the listing of the stock of the Provider on any recognised stock exchange.
- 11.4 The provisions of this Clause 11 shall continue in force for a period of 3 years following the termination of this Agreement, at the end of which period they will cease to have effect.

12. Data protection

- 12.1 Each party shall comply with the Data Protection Laws with respect to the processing of the Customer Personal Data.
- 12.2 The Customer confirms to the Provider that it has the legal right to disclose all Personal Data that it does in fact disclose to the Provider under or in connection with this Agreement.
- 12.3 The Provider warrants to the Customer that the Customer Personal data is processed and stored within the United Kingdom, including any personal data which is processed by the Providers sub-processor(s), subject to the notice noted in Schedule 3, Clause 7. Transfer of the Customer Personal Data outside the United Kingdom will only occur in accordance with Clause 12.6.
- The Customer shall only supply to the Provider, and the Provider shall only process, in each case under or in relation to this Agreement, the Personal Data of data subjects falling within the categories specified in Part 1 of Schedule 3 (Data processing information) and of the types specified in Part 2 of Schedule 3 (Data processing information); and the Provider shall only process the Customer Personal Data for the purposes specified in Part 3 of Schedule 3 (Data processing information).
- 12.4 The Provider shall only process the Customer Personal Data during the Term, subject to the other provisions of this Clause 12.



- 12.5 The Provider shall only process the Customer Personal Data on the documented instructions of the Customer (including with regard to transfers of the Customer Personal Data to any place outside the United Kingdom).
- 12.6 The Provider shall promptly inform the Customer if, in the opinion of the Provider, an instruction of the Customer relating to the processing of the Customer Personal Data infringes the Data Protection Laws.
- 12.7 Notwithstanding any other provision of this Agreement, the Provider may process the Customer Personal Data if and to the extent that the Provider is required to do so by applicable law. In such a case, the Provider shall inform the Customer of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
- 12.8 The Provider shall ensure that persons authorised to process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- 12.9 The Provider and the Customer shall each implement appropriate technical and organisational measures to ensure an appropriate level of security for the Customer Personal Data.
- 12.10 The Provider must not engage any third party to process the Customer Personal Data without the prior specific or general written authorisation of the Customer. In the case of a general written authorisation, the Provider shall inform the Customer at least 14 days in advance of any intended changes concerning the addition or replacement of any third party processor, and if the Customer objects to any such changes before their implementation, then the Provider must not implement the changes. The Provider shall ensure that each third party processor is subject to the same legal obligations as those imposed on the Provider by this Clause 12 and shall be responsible for the acts and/or omissions of said third party processor.
- 12.11 The Provider shall, insofar as possible and taking into account the nature of the processing, take appropriate technical and organisational measures to assist the Customer with the fulfilment of the Customer's obligation to respond to requests exercising a data subject's rights under the Data Protection Laws.
- 12.12 The Provider shall assist the Customer in ensuring compliance with the obligations relating to the security of processing of personal data, the notification of personal data breaches to the supervisory authority, the communication of personal data breaches to the data subject, data protection impact assessments and prior consultation in relation to high-risk processing under the Data Protection Laws. The Provider shall report any Personal Data breach relating to the Customer Personal Data to the Customer within 24



hours following the Provider becoming aware of the breach. The Provider may charge the Customer any reasonable expenses incurred for any work performed by the Provider at the request of the Customer pursuant to this Clause 12.13. Reasonable evidence of such expenditure must be provided to the Customer.

- 12.13 The Provider shall make available to the Customer all information necessary to demonstrate the compliance of the Provider with its obligations under this Clause 12 and the Data Protection Laws.
- 12.14 The Provider shall, at the choice of the Customer, delete or return all of the Customer Personal Data to the Customer after the provision of services relating to the processing, and shall delete existing copies save to the extent that applicable law requires storage of the relevant Personal Data and if this is required, the Customer will be notified of this in writing by the Provider.
- 12.15 The Provider shall allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer in respect of the compliance of the Provider's processing of Customer Personal Data with the Data Protection Laws and this Clause 12. The Provider may charge the Customer at its standard time-based charging rates for any work performed by the Provider at the request of the Customer pursuant to this Clause 12.16.
- 12.16 If any changes or prospective changes to the Data Protection Laws result or will result in one or both parties not complying with the Data Protection Laws in relation to processing of Personal Data carried out under this Agreement, then the parties shall use their best endeavours promptly to agree such variations to this Agreement as may be necessary to remedy such non-compliance.

13. Dispute Resolution

- 13.1 In the event of a dispute arising out of or in relation to the terms of this Agreement, representatives of Provider and Customer shall meet and endeavour to settle the dispute in an amicable manner through mutual consultation. If such persons are unable to resolve the dispute in a satisfactory manner within fourteen (14) days of such meeting, either party may give the other notice to seek to resolve the dispute or difference through an Alternative Dispute Resolution (ADR) procedure in accordance with the mediation procedure of the Centre for Effective Dispute Resolution (CEDR).
- 13.2 If the parties fail to agree terms of settlement of their dispute or difference within 56 days of the receipt of such notice or the party to whom the notice was given refuses to participate in the ADR procedure then the matter shall be referred to Arbitration in accordance with Clause 13.3.



13.3 Subject to Clause 13.4 below if any dispute or difference which may arise between the parties in connection with or arising out of the Agreement is referred to ADR mediation but is not so settled as specified in this Clause 13, then either party shall give notice to the other and such dispute or difference shall be referred to Arbitration. The parties shall agree on the appointment of a single arbitrator within fourteen (14) days after the date of such notice or in default of agreement the arbitrator shall be nominated on the application of either party by the President for the time being of the Chartered Institute of Arbitrators. The Arbitration shall be conducted in accordance with the then current Arbitration Rules as published by the Chartered Institute of Arbitrators.

13.4 There are excluded from Arbitration any proceedings brought by one party against the other which arise out of the failure by that other party to comply with the provisions of any binding agreement setting out the terms upon which the dispute or difference was settled as a result of or following from the ADR mediation procedure referred to in Clause 13.1 above.

14. Warranties and Indemnities

14.1 The Provider warrants to the Customer that:

- (a) the Provider has the legal right and authority to enter into this Agreement and to perform its obligations under this Agreement;
- (b) it has and will maintain all necessary licences, consents and permissions necessary for the performance of its obligations under this Agreement;
- (c) the Provider will comply with all applicable legal and regulatory requirements applying to the exercise of the Provider's rights and the fulfilment of the Provider's obligations under this Agreement;
- (d) the Provider has or has access to all necessary know-how, expertise and experience to perform its obligations under this Agreement; and
- (e) the information provided to the Customer prior to the Effective Date on the security of the Provider's network and information systems is up to date and accurate.
- (f) it will co-operate with the Customer in all matters relating to the Services and comply with the Customer's reasonable instructions;
- (g) it will not do or omit to do anything which may cause the Customer to lose any licence, authority, consent, or permission on which it relies for the purposes of conducting its business; and



- (h) it will notify the Customer in writing immediately upon the occurrence of a change of control of the Provider.

14.2 The Provider warrants to the Customer that:

- (a) the Platform and Hosted Services will conform in all material respects with the Hosted Services Specification;
- (b) to the best of our endeavours the Hosted Services will be free from Hosted Services Defects;
- (c) to the best of our endeavours the application of Updates and Upgrades to the Platform by the Provider will not introduce any Hosted Services Defects into the Hosted Services;
- (d) the Platform will be free from Viruses, ransomware, spyware, adware, and other malicious software programs; and
- (e) the Platform will incorporate security features reflecting the requirements of good industry practice.

14.3 The Provider warrants to the Customer that the Hosted Services and Platform, when used by the Customer in accordance with this Agreement, will not breach any laws, statutes or regulations applicable under English law.

14.4 The Provider warrants to the Customer that the Hosted Services and Platform, when used by the Customer in accordance with this Agreement, will not infringe the Intellectual Property Rights of any person in any jurisdiction and under any applicable law.

14.5 The Provider shall defend the Customer against any and all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses suffered or incurred or paid by the Customer arising out of or in connection with any claim brought against the Customer for actual or alleged infringement of a third party's intellectual property rights associated with the Customer's use of the Provider's Hosted Service.

14.6 If the Provider reasonably determines, or any third party alleges, that the use of the Hosted Services by the Customer in accordance with this Agreement infringes any person's Intellectual Property Rights, the Provider may at its own cost and expense:

- (a) modify the Hosted Services in such a way that they no longer infringe the relevant Intellectual Property Rights; or



- (b) procure for the Customer the right to use the Hosted Services in accordance with this Agreement.

14.7 The Customer warrants to the Provider that it has the legal right and authority to enter into this Agreement and to perform its obligations under this Agreement.

14.8 All the parties' warranties and representations in respect of the subject matter of this Agreement are expressly set out in this Agreement. To the maximum extent permitted by applicable law, no other warranties or representations concerning the subject matter of this Agreement will be implied into this Agreement or any related contract.

15. Acknowledgements and warranty limitations

15.1 The Customer acknowledges that complex software is never wholly free from defects, errors and bugs; and subject to the other provisions of this Agreement, the Provider gives no warranty or representation that the Hosted Services will be wholly free from defects, errors and bugs.

15.2 The Customer acknowledges that complex software is never entirely free from security vulnerabilities; and subject to the other provisions of this Agreement, the Provider gives no warranty or representation that the Hosted Services will be entirely secure. Nothing in this Agreement shall override the Provider and/or Customer obligations under the Data Protection Laws or the provisions of Clause 11 or Clause 12.

15.3 The Customer acknowledges that the Hosted Services are designed to be compatible only with that software and those systems specified as compatible in the Hosted Services Specification; and the Provider does not warrant or represent that the Hosted Services will be compatible with any other software or systems.

16. Limitations and exclusions of liability

16.1 Nothing in this Agreement will:

- (a) limit or exclude any liability for death or personal injury resulting from negligence;
- (b) limit or exclude any liability for fraud or fraudulent misrepresentation;
- (c) limit any liabilities in any way that is not permitted under applicable law; or
- (d) exclude any liabilities that may not be excluded under applicable law.
- (e) limit the Providers liability under Clause 14.4.

16.2 The limitations and exclusions of liability set out in this Clause 16 and elsewhere in this Agreement:



- (a) are subject to Clause 16.1; and
 - (b) govern all liabilities arising under this Agreement or relating to the subject matter of this Agreement, including liabilities arising in contract, in tort (including negligence) and for breach of statutory duty, except to the extent expressly provided otherwise in this Agreement.
- 16.3 Neither party shall be liable to the other party in respect of any losses arising out of a Force Majeure Event.
- 16.4 Neither party shall be liable to the other party in respect of any loss of profits or anticipated savings.
- 16.5 Neither party shall be liable to the other party in respect of any loss of revenue or income.
- 16.6 Neither party shall be liable to the other party in respect of any loss of business, contracts or opportunities.
- 16.7 Neither party shall be liable to the other party in respect of any loss or corruption of any data, database or software; providing that this Clause 16.7 shall not protect the Provider unless the Provider has fully complied with its obligations under Clause 7.3 and Clause 7.4. and neither will protection extend to any breach of Clause 11 or Clause 12.
- 16.8 Neither party shall be liable to the other party in respect of any special, indirect, or consequential loss or damage.
- 16.9 The liability of each party to the other party under this Agreement in respect of any event or series of related events shall not exceed the greater of:
- (a) £10,000; and
 - (b) the total amount paid and payable by the Customer to the Provider under this Agreement in the 12 month period preceding the commencement of the event or events.
 - (c) The provider shall have a higher liability cap of one million pounds regarding any breach of Data Protection Laws or the provisions of Clause 11 and Clause 12.
- 16.10 The aggregate liability of each party to the other party under this Agreement shall not exceed the total amount paid and payable by the Customer to the Provider under this Agreement. Where the liability is in respect of any breach of Data Protection Laws or the provisions of Clause 11 and Clause 12 the aggregate liability will be one million pounds.



17. Force Majeure Event

- 17.1 If a Force Majeure Event gives rise to a failure or delay in either party performing any obligation under this Agreement (other than any obligation to make a payment), that obligation will be suspended for the duration of the Force Majeure event.
- 17.2 A party that becomes aware of a Force Majeure Event which gives rise to, or which is likely to give rise to, any failure or delay in that party performing any obligation under this Agreement, must:
- (a) promptly notify the other; and
 - (b) inform the other of the period for which it is estimated that such failure or delay will continue.
- 17.3 A party whose performance of its obligations under this Agreement is affected by a Force Majeure Event must take reasonable steps to mitigate the effects of the Force Majeure Event.

18. Termination

- 18.1 Either party may terminate this Agreement by giving to the other party not less than **sixty days'** written notice of termination, prior to any anniversary of the Effective Date of this Agreement.
- 18.2 Either party may terminate this Agreement immediately by giving written notice of termination to the other party if the other party commits a material breach of this Agreement.
- 18.3 Either party may terminate this Agreement immediately by giving written notice of termination to the other party if:
- (a) the other party:
 - (i) is dissolved;
 - (ii) ceases to conduct all (or substantially all) of its business;
 - (iii) is or becomes unable to pay its debts as they fall due;
 - (iv) is or becomes insolvent or is declared insolvent; or
 - (v) convenes a meeting or makes or proposes to make any arrangement or composition with its creditors;
 - (b) an administrator, administrative receiver, liquidator, receiver, trustee,



manager or similar is appointed over any of the assets of the other party;

- (c) an order is made for the winding up of the other party, or the other party passes a resolution for its winding up (other than for the purpose of a solvent company reorganisation where the resulting entity will assume all the obligations of the other party under this Agreement).

19. Effects of termination

19.1 Upon the termination of this Agreement, all of the provisions of this Agreement shall cease to have effect, save that the following provisions of this Agreement shall survive and continue to have effect (in accordance with their express terms or otherwise defined): Clauses 1, 4.11, 10.2, 10.4, 11, 12.1, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13, 12.14, 12.15, 12.16, 12.17, 16, 19, 22 and 23.

19.2 Except to the extent that this Agreement expressly provides otherwise, the termination of this Agreement shall not affect the accrued rights of either party.

19.3 Within 30 days following the termination of this Agreement for any reason the Customer must pay to the Provider any Charges in respect of Services provided to the Customer before the termination of this Agreement.

19.4 The initial Hosted Service period and subsequent Hosted Service periods run for a full twelve months and early termination in accordance with clause 18 does not entitle the Customer to a refund, or credit, for any unused time of the Hosted Service, unless the Customer terminates the Agreement early on the basis of a material breach of any term of this Agreement by the Provider, or if the Provider terminates the Agreement early on the basis of convenience (in accordance with Clause 18.1) in which case the Customer shall be entitled to such refund or credit for any unused time.

20. Notices

20.1 Any notice from one party to the other party under this Agreement must be given by one of the following methods (using the relevant contact details set out in Clause 20.2 and Part 3 of Schedule 1 (Hosted Services Particulars)):

- (a) delivered personally or sent by courier, in which case the notice shall be deemed to be received upon delivery; or
- (b) sent by recorded signed-for post, in which case the notice shall be deemed to be received 2 Business Days following posting,

providing that, if the stated time of deemed receipt is not within Business Hours, then the time of deemed receipt shall be when Business Hours next begin after the



stated time.

- 20.2 The Provider's contact details for notices under this Clause 20 are as follows:
The Company Secretary, Vantage Technologies Limited, Vantage House, Rother Valley Way, Sheffield, S20 3RW.
- 20.3 The addressee and contact details set out in Clause 20.2 and Part 3 of Schedule 1 (Hosted Services particulars) may be updated from time to time by a party giving written notice of the update to the other party in accordance with this Clause 20.

21. Subcontracting

- 21.1 The Provider must not subcontract any of its obligations under this Agreement without the prior written consent of the Customer, providing that the Customer must not unreasonably withhold or delay the giving of such consent.
- 21.2 The Provider shall remain responsible to the Customer for the performance of any subcontracted obligations.
- 21.3 Notwithstanding the provisions of this Clause 21 but subject to any other provision of this Agreement, the Customer acknowledges and agrees that the Provider may subcontract to any reputable third party hosting business the hosting of the Platform and the provision of services in relation to the support and maintenance of elements of the Platform.

22. General

- 22.1 No breach of any provision of this Agreement shall be waived except with the express written consent of the party not in breach.
- 22.2 If any provision of this Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions of this Agreement will continue in effect. If any unlawful and/or unenforceable provision would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect (unless that would contradict the clear intention of the parties, in which case the entirety of the relevant provision will be deemed to be deleted).
- 22.3 This Agreement may not be varied except by a written document signed by or on behalf of each of the parties.
- 22.4 Neither party may without the prior written consent of the other party assign, transfer, charge, license or otherwise deal in or dispose of any contractual rights or obligations under this Agreement.



- 22.5 This Agreement is made for the benefit of the parties, and is not intended to benefit any third party or be enforceable by any third party. The rights of the parties to terminate, rescind, or agree any amendment, waiver, variation or settlement under or relating to this Agreement are not subject to the consent of any third party.
- 22.6 Subject to Clause 16.1, this Agreement shall constitute the entire agreement between the parties in relation to the subject matter of this Agreement, and shall supersede all previous agreements, arrangements and understandings between the parties in respect of that subject matter.
- 22.7 This Agreement shall be governed by and construed in accordance with English law.
- 22.8 The courts of England shall have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this Agreement.

23. Interpretation

- 23.1 In this Agreement, a reference to a statute or statutory provision includes a reference to:
- (a) that statute or statutory provision as modified, consolidated and/or re-enacted from time to time; and
 - (b) any subordinate legislation made under that statute or statutory provision.
- 23.2 The Clause headings do not affect the interpretation of this Agreement.
- 23.3 References in this Agreement to "calendar months" are to the 12 named periods (January, February and so on) into which a year is divided.
- 23.4 In this Agreement, general words shall not be given a restrictive interpretation by reason of being preceded or followed by words indicating a particular class of acts, matters or things.



EXECUTION

The parties have indicated their acceptance of this Agreement by executing it below.

SIGNED BY: Anthony Mitcheson
duly authorised for and on behalf of the Provider

Date: 2024

SIGNED BY:
duly authorised for and on behalf of the Customer

Date:



SCHEDULE 1 (HOSTED SERVICES PARTICULARS)

Part 1. Specification of Hosted Services

Vantage Enterprise Hosted Service that includes the following modules:

Asset and Facilities Management and Maintenance, Audit and Inspection, Central Safety Alerts, Complaints and Compliments, Compliance Management (CQC, HIS, RQIA, HIW), Contract Management and Staff Lists, COSHH and Risk Assessments, Daily Records and Goal Setting, DPIA, Display Screen Assessments, Event Management, File Store, Goal Setting and Management, Good Practice Reporting, GDPR (Register of Process Activity – ROPA), Health & Safety, Helpdesk/Support, HR, Incident Management, PPM (Planned Preventative Maintenance), Policy Management, Practices and Privileges, Risk Management, Safeguarding, Service User Records, Subject Access Requests (SAR), Supervision, Surveys and Feedback, Training Management, Vehicle Management, Volunteer Management.

Additional services: (if applicable)

Part 2. Financial provisions

a. Initial Hosted Service Charge

The initial Hosted Service charge is **£xxxxxxx.xx** plus VAT, which shall be invoiced by the Provider upon receipt of order for the Hosted Service.

b. Subsequent Hosted Service Charge

The subsequent Hosted Service Charge will be the same as the initial Hosting Service Charge, increased annually in line the Retail Prices Index (all items) published by the UK Office for National Statistics, which shall be invoiced by the Provider thirty days prior to expiry of the initial Hosting Service period unless terminated by the Customer in accordance with clause 18.

c. Other Charges

- i. In addition to the Hosted Service Charges detailed above, the Provider will invoice in respect of, and the Customer shall pay to the Provider all other Charges that are agreed between the parties in writing from time to time.
- ii. Where other charges are to be calculated by reference to a daily or hourly rate, the following rates shall apply as at the date of this Agreement:



Development charges	£750	Daily rate
Training charges	£750	Daily rate
Return of stored data	£750	Daily rate
Small Jobs	£ 92	Hourly rate

The above rates may increase annually in line the Retail Prices Index (all items) published by the UK Office for National Statistics.

d. Expenses

- i. The following expenses may be passed on by the Provider to the Customer at cost, subject to the prior approval of the Customer:

Travel expenses

Accommodation expenses

Subsistence expenses.

- ii. The expenses may be invoiced by the Provider to the Customer at any time after the relevant expense has been incurred.

Part 3. Contractual notices

The Chief Executive
XXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXX

Part 4. Service Level Agreement

The Provider will:

- (a) respond to requests for Support Services made through the helpdesk; and
- (b) resolve issues raised by the Customer in accordance with the following response time matrix.



Severity	Examples	Response time	Resolution time
Critical	Complete system failure; permanent data loss; unrelated applications malfunction; most common operations fail consistently.	3 elapsed hours	1 working day or Continuous effort
High	Major function has reproducible problem; major inconvenience; common operations fail consistently; application fails readily.	6 elapsed hours	7 working days
Medium	Important function has intermittent problem; common operation fails occasionally; occasional operation fails consistently.	2 working days	14 working days
Low	Occasional operation fails intermittently; cosmetic errors; user guidance.	5 working days	Open / next release

- 3.2 The Provider will determine, acting reasonably, in to which severity category an issue raised through the Support Services falls.
- 3.3 All Support Services will be provided remotely unless expressly agreed otherwise by the Provider.
- 3.4 A persistent failure to meet critical or high service levels will amount to a material breach under clause 19.2.
- 3.5 Any failure of the Provider to meet the required response and/or resolution times in accordance with the following, will be deemed a material breach of this Agreement by the Provider, entitling the Customer to terminate the Agreement:
- (a) within any given seven day period, in relation to two or more service calls made within the critical and/or high severity levels; and/or
 - (b) three or more service calls within the medium severity level within any given seven day period.

SCHEDULE 2 (ACCEPTABLE USE POLICY)

1. Introduction

- 1.1 This acceptable use policy (the "**Policy**") sets out the rules governing:
- (a) the use of the website at www.vantage-modules.co.uk any successor website, and the services available on that website or any successor



website (the "**Services**"); and

- (b) the transmission, storage, and processing of content by you, or by any person on your behalf, using the Services ("**Content**").

1.2 References in this Policy to "you" are to any customer for the Services and any individual user of the Services (and "your" should be construed accordingly); and references in this Policy to "us" are to Vantage Technologies Limited (and "we" and "our" should be construed accordingly).

1.3 By using the Services, you agree to the rules set out in this Policy.

1.4 We will ask for your express agreement to the terms of this Policy before you login to use the Services.

2. General usage rules

2.1 You must not use the Services in any way that causes, or may cause, damage to the Services or impairment of the availability or accessibility of the Services.

2.2 You must not use the Services:

- (a) in any way that is unlawful, illegal, fraudulent, deceptive, or harmful; or
- (b) in connection with any unlawful, illegal, fraudulent, deceptive, or harmful purpose or activity.

2.3 You must ensure that all Content complies with the provisions of this Policy.

3. Unlawful Content

3.1 Content must not be illegal or unlawful, must not infringe any person's legal rights, and must not be capable of giving rise to legal action against any person (in each case in any jurisdiction and under any applicable law).

3.2 Content must not:

- (a) be libelous or maliciously false;
- (b) be obscene or indecent;
- (c) infringe any copyright, moral right, database right, trademark right, design right, right in passing off, or other intellectual property right;
- (d) infringe any right of confidence, right of privacy or right under data protection legislation;
- (e) constitute negligent advice or contain any negligent statement;



- (f) constitute an incitement to commit a crime, instructions for the commission of a crime or the promotion of criminal activity;
- (g) be in contempt of any court, or in breach of any court order;
- (h) constitute a breach of racial or religious hatred or discrimination legislation;
- (i) be blasphemous;
- (j) constitute a breach of official secrets legislation; or
- (k) constitute a breach of any contractual obligation owed to any person.

3.3 You must ensure that Content is not and has never been the subject of any threatened or actual legal proceedings or other similar complaint.

4. Graphic material

4.1 Content must not depict violence in an explicit, graphic, or gratuitous manner save as far CCTV footage which may need to be uploaded in support of an incident.

4.2 Content must not be pornographic or sexually explicit.

5. Factual accuracy

5.1 Content must not be untrue, false, inaccurate or misleading.

5.2 Statements of fact contained in Content and relating to persons (legal or natural) must be true; and statements of opinion contained in Content and relating to persons (legal or natural) must be reasonable, be honestly held and indicate the basis of the opinion.

6. Etiquette

6.1 Content must be appropriate, civil and tasteful, and accord with generally accepted standards of etiquette and behaviour on the internet.

6.2 Content must not be offensive, deceptive, threatening, abusive, harassing, menacing, hateful, discriminatory or inflammatory.

6.3 You must not use the Services to send any hostile communication or any communication intended to insult, including such communications directed at a particular person or group of people.

6.4 You must not use the Services for the purpose of deliberately upsetting or offending



others.

6.5 You must not unnecessarily flood the Services with material relating to a particular subject or subject area, whether alone or in conjunction with others.

6.6 You must ensure that Content does not duplicate other content available through the Services.

6.7 You must ensure that Content is appropriately categorised.

6.8 You should use appropriate and informative titles for all Content.

6.9 You must always be courteous and polite to other users of the Services.

7. Marketing and spam

7.1 You must not use the Services for any purpose relating to the marketing, advertising, promotion, sale or supply of any product, service or commercial offering.

7.2 Content must not intentionally constitute or contain spam, and you must not use the Services to store or transmit spam – which for these purposes shall include all unlawful marketing communications and unsolicited commercial communications.

7.3 You must not send any spam or other marketing communications to any person using any email address or other contact details made available through the Services or that you find using the Services.

7.4 You must not use the Services to promote, host or operate any chain letters, Ponzi schemes, pyramid schemes, matrix programs, multi-level marketing schemes, "get rich quick" schemes or similar letters, schemes or programs.

7.5 You must not use the Services in any way which is liable to result in the blacklisting of any of our IP addresses.

8. Monitoring

8.1 You acknowledge that we may actively monitor the Content and the use of the Services.

9. Data mining

9.1 You must not conduct any systematic or automated data scraping, data mining, data extraction or data harvesting, or other systematic or automated data collection activity, by means of or in relation to the Services without the prior written consent of the Provider.



10. Hyperlinks

- 10.1 You must not link to any material using or by means of the Services that would, if it were made available through the Services, breach the provisions of this Policy.

11. Harmful software

- 11.1 The Content must not contain or consist of, and you must not promote, distribute or execute by means of the Services, any viruses, worms, spyware, adware or other harmful or malicious software, programs, routines, applications or technologies.
- 11.2 The Content must not contain or consist of, and you must not promote, distribute or execute by means of the Services, any software, programs, routines, applications or technologies that will or may have a material negative effect upon the performance of a computer or introduce material security risks to a computer.



SCHEDULE 3 (DATA PROCESSING INFORMATION)

1. The Customer is the Data Controller, and the Provider is the Data Processor

2. Categories of data subject

Any individual who is the subject of Personal Data

3. Types of Personal Data

Names and addresses of patients, service users, customers, supporters, volunteers, contractors, and staff, addresses and dates of birth of individuals in connection with health and safety reports/incidents.

For patients and service users NHS Number, telephone number(s), email addresses, names of relatives and carers, date of birth, and GP surgery will also be stored.

Special category data relating to a patients' and service users' health, sex life and/or sexual orientation may also be stored.

4. Purposes of processing

Personal data will be processed for the purposes of incident and complaint management, risk monitoring, health and safety, and Data Protection law compliance.

Data will be processed under the following categories and for the following purposes.

Contractual Necessity – Art.6(1)(b) of UK GDPR – the processing is necessary for a contract with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation: Art.6(1)(c) of UK GDPR the processing is necessary to comply with the law (not including contractual obligations).

Public task: Art.6(1)(e) of UK GDPR the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

Special category data will be processed for lawful basis under UK GDPR Article 9(2)(b) – processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of



employment and social security and social protection law insofar as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

Article 9(2)(h) – **Health and Social Care with a basis in law.**

5. Duration of processing

For the duration of this contract

6. Security measures for Personal Data

The policies and procedures associated with the Providers Information Security Management System.

7. Sub-processors of Personal Data

Microsoft – Azure cloud computing platform that gives access to cloud services and resources provided by Microsoft. These services and resources include storing data.

Twilio SendGrid – customer communication platform for transactional emails sent from Vantage Software.

Twilio is certified to participate in the UK Extension to the EU-US Data Privacy Framework and may received personal data from the United Kingdom in reliance on the UK Extension to the EU-US Data Privacy Framework effective 12th October 2023, which is the date of entry into force of the adequacy regulations implementing the data bridge for the UK Extension to the EU-US Data Privacy Framework. The data bridge for the UK Extension to the EU-US Data Privacy Framework enables the transfer of United Kingdom personal data to participating organisations consistent with United Kingdom law.