Private & Confidential

DATED

June 2021

DEPARTMENT OF HEALTH AND SOCIAL CARE (1)

and

UGENTEC NV LIMITED

(2)

# SOFTWARE LICENCE AND SUPPORT AGREEMENT

# **CONTENTS**

Clause	Heading Pag	е
1	Definitions 1	l
2	Commencement and Duration	)
3	Software and Services to be provided by the Supplier	)
4	General Obligations of the Supplier10	)
5	Undertakings and Representations10	)
6	Change Control Procedure11	L
7	Price & Payment12	2
8	Service Credits13	3
9	Intellectual Property Rights14	1
10	Data Protection	7
11	Employees	3
12	Insurance	)
13	Liability and Indemnities19	)
14	Compliance with Laws and Customer Policies	)
15	Contract Management and Audit20	)
16	Confidentiality22	2
17	Force Majeure	3
18	Termination	1
19	Consequences of Termination25	
20	Assignment, Subcontracting and Third Party Rights	5
21	Entire Agreement27	
22	Financial standing of Supplier28	3
23	General	)
24	Bribery & Gifts31	
25	Notices	
26	Dispute Resolution Procedure	3
27	Law	
28	Jurisdiction 34	
Schedule 1	Specification	÷
Schedule 2	Support Services	
Schedule 3	Part A - Service Levels and Service Credits	
Schedule 4	Security Undertakings71	l
Schedule 5	Charges	
Schedule 8	Approved Sub-Contractors78	3

|

#### 11-6-2021

THIS AGREEMENT is made on [INSERT HERE DATE OF SIGNATURE - DO NOT INSERT AN EARLIER DATE] BETWEEN

- (1) The Secretary of State for Health and Social Care of 39 Victoria St, Westminster, London SW1H 0EU acting as part of the Crown through the Department of Health and Social Care (the "Customer"); and
- (2) UgenTec NV Limited (a company registered in Belgium No. 0551.976.421) whose registered office is at Kempische Steenweg 303/105, Hasselt 3500, Belgium (the "Supplier").

### BACKGROUND

- (A) As part of HM Government's emergency response to the Covid-19 pandemic, the Customer has a requirement for Software and Services to support high-capacity diagnostic testing using end-point polymerase chain reaction (EPCR) assay technology.
- (B) Following the successful completion of user acceptance tests on the Software, the Customer wants to appoint the Supplier as supplier of the Software and Services.
- (C) The Parties wish to enter this Agreement to regulate the terms and conditions on which the Supplier is to provide the Software and the Services to Customer.

### THE PARTIES AGREE as follows:

### 1 <u>Definitions</u>

1.1. In this Agreement:

"Agreement" means this agreement together with all of its schedules, attachments, exhibits and appendices as from time to time amended or supplemented and any document which amends or supplements this Agreement;

"Applicable Laws" means all applicable laws, legislation, European regulations, statutes, statutory instruments, regulations, edicts, by-laws or directions or guidance from government or governmental agencies which have the force of law whether local, national, international or otherwise existing from time to time and as far as applicable to the use of the Software and receipt of the Services by the Customer and/or the End User;

"Approved Sub-Contractors" means the sub-contractors set out in Schedule 8 (Approved Sub-Contractors);

"Audit Agents" means any of the Customer's internal and external auditors; the Customer's statutory or regulatory auditors; the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; HM Treasury or the Cabinet Office; any party formally appointed by the Customer to carry out audit or similar review functions; and successors or assigns of any of the above;

"Authorised Representative" means the person(s) designated as such by Customer and the Supplier and notified as such to the other Party in writing from time to time;

"Bank Guarantee" has the meaning set out in Clause 22.3;

"Baseline Personal Security Standard (BPSS)" defined by HMG in the following document: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard

"Bribery Act" means the Bribery Act 2010 as amended and including any legislation amending or replacing the same;

"Bribery Offence" has the meaning set out in Clause 24.1;

"Business Day" means any day which is not a Saturday, a Sunday or a bank or public holiday in England;

**"Change Control Procedure"** means the procedure for the proper management of changes during the term of this Agreement set out in Clause 6;

"Change of Control" means that the person who controlled or had the power to control the affairs and policies of the applicable company (whether directly or indirectly and either by ownership or share capital, possession of voting power, ability to appoint directors, contract or otherwise) ceases to have such control;

"Change Request" has the meaning set out in Clause 6.1;

"Charges" means the charges set out in Schedule 4 (Charges);

"Commencement Date" means April 27th, 2021;

"Confidential Information" means the provisions of this Agreement and all information in any form or medium which is secret or otherwise not publicly available (either in its entirety or in part including the configuration or assembly of its components) including commercial, financial, marketing, or technical information, know-how, trade secrets, business methods and other information in any form or medium whether disclosed orally or in writing before or after the date of this Agreement, together with any reproductions of such information in any form or medium or any part(s) of this information;

"Critical Error" means:

(a) An Error, Defect or Omission which causes the licenced software to be unusable; or

(b) A breach of availability targets for three (3) consecutive months;

**"Critical Service Level Failure"** means either the occurrence of three (3) Critical Errors within any period of three (3) consecutive Months during the Agreement;

"Customer Affiliate" means each member of the Customer Group, any contractual joint venture to which Customer is a Party and any joint venture in which Customer has a controlling interest whether through the ownership of shares or board control, and any Customer franchisee from time to time;

"Customer Contract Manager" means or such other person notified in writing by Customer to the Supplier;

"Customer Standards" means a published statement or set of requirements on a topic specifying the characteristics, usually measurable, that must be satisfied or achieved to comply with the standard.

**"Data"** shall mean the personal data and special category personal data (as both terms are defined in the UK GDPR) provided by the Customer to the Supplier pursuant to this Agreement or which is otherwise Processed by the Supplier on behalf of the Customer pursuant to this Agreement;

"Data Protection Laws" means the DPA 2018, the EU GDPR, the UK GDPR, the Law Enforcement Directive (Directive (EU) 2016/680) as transposed into the law of England and Wales, Scotland and Northern Ireland by virtue of Part 3 of the DPA 2018 and any other national legislation and related statutory instruments relating to privacy and the protection of personal data as amended or in force from time to time;

"Defect" means any defect or deficiency in the Software which renders it unable to:

- (a) perform the functions or to meet the performance standards set out in the relevant Specification; and/or
- (b) comply with the requirements of this Agreement;

**"Developed Work"** means any work of whatsoever nature which is produced for, on behalf of, or at the request of Customer pursuant to this Agreement and that is explicitly identified as developed work by the Parties, excluding any Pre-Existing Rights of the Supplier and any improvements hereto;

**"Disabling Device"** means any program routine or device which is designed to delete, disable, deactivate, interfere with or otherwise harm any Customer computer, server, mainframe or computer system, including any virus, timebomb, software lock, drop-dead device, malicious logic, worm, trojan horse or trap door;

"Documentation" means any description of the Software, the Specification and all technical specifications, End User manuals, operating manuals, process definitions and procedures relating thereto;

"Downtime" means any period of time during which FastFinder is not available for access or use by the End User;

**"DPA 2018"** means the Data Protection Act 2018 as modified by Schedule 2 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019;

**"End User"** means any natural person or legal entity that has been authorised by the Customer to use FastFinder / the Supplier platform under the responsibility of the Customer and/or in such Customer's name and/or on such Customer's behalf;

"Escrow Agreement" has the meaning given to it in Clause 22.4;

**"EU GDPR"** means the regulations on the protection of natural persons with regard to the processing of personal data and on the free movement of such data known as the General Data Protection Regulation (EU) 2016/679;

"Extension Period" has the meaning given to it in Clause 2.2;

**"Force Majeure"** means any event outside the reasonable control of either Party affecting its ability to perform any of its obligations under this Agreement including but not limited to Act of God, fire, flood, war, revolution, acts of terrorism, riot or civil commotion and trade embargo, but excluding severe weather and strikes, lock-outs or other industrial action (whether of the affected Party's own employees or others);

"Foreign Bribery Conduct" means any conduct, whether by act or omission, which did not constitute a Bribery Offence but which would have constituted a Bribery Offence if it had been engaged in or carried out in the United Kingdom or been engaged in or carried out outside the United Kingdom by a British citizen, a British overseas territories citizen, a British National (Overseas), a British Overseas citizen, a person who under the British Nationality Act 1981 (the "BNA") was a British subject, a British protected person within the meaning of the BNA, an individual ordinarily resident in the United Kingdom, a body incorporated under the law in any part of the United Kingdom or a Scottish partnership;

"Good Industry Practice" means the exercise of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced operator engaged in the same type of undertaking and under the same or similar circumstances and conditions, seeking in good faith to comply with its contractual obligations, complying with all Applicable Laws, rules and regulations including codes of practice and conduct in force from time to time; "Group" means in relation to any company that company and every other company which from time to time is or becomes a subsidiary or holding company of that company or a subsidiary of any such holding company (and the terms "subsidiary" and "holding company" shall have the meanings given to them by Section 1159 of the Companies Act 2006);

"Incident" means a reported occurrence of a failure to deliver any part of the Services in accordance with the specification as outlined in Schedule 1;

"Information Assurance" means measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

"Information Security Management System" An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data.

"Intellectual Property Right" means any intellectual property rights including patents, utility models, designs, design rights, copyright (including rights in software), decryption rights, database rights, trade marks, rights pursuant to passing off, service marks, domain names, know-how, rights in confidential information (including technical and commercial trade secrets) and image rights, in each case whether registered or not and including any application for registration and renewals or extensions of such rights in any country in the world;

"Key Personnel" mean any sub-contractor of the Supplier and the Supplier's officers, employees, agents, consultants and sub-contractors and any other persons who provide or are involved in the provision of the Services;

"Laboratory Operator" means the party operating the laboratory at the Locations from time to time;

"Locations" means the locations at which the Software is to be installed, details of which are set out in Schedule 1 (Specification), provided that Customer shall be free in its absolute discretion to amend that list of Locations by notice in writing to the Supplier;

"Marks" means all logos, trade names and/or trade marks (whether registered or not) owned or used by Customer in the course of its business;

"Material Service Level Breach" has the meaning set out in Schedule 3 (Service Levels & Service Credits);

"Monthly Uptime Percentage" has the meaning set out in Schedule 3 (Service Levels & Service Credits);

"Object Code" means the binary programming language capable of being understood by a computer;

"Omission" means a failure by the Supplier to do something whether through negligence or otherwise;

**"Open Book Data"** complete and accurate financial and non-financial information which is sufficient to enable the Customer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the term of the Agreement, including details and all assumptions relating to:

- (a) Number of tests performed and calculation of Charges according to Schedule 5;
- (b) Records and calculations regarding Service Credits;
- (c) Records and calculations regarding Developed Work that is assigned by the Supplier to the Customer as set out in Clause 9.11.; and
- (d) Records and calculations regarding Change Requests.

"Party" means Customer or the Supplier as the context dictates and "Parties" means both Customer and the Supplier;

"Pre-Existing Rights" means Intellectual Property Rights that are controlled by the Supplier as at the date of this Agreement;

"Process", "Processing" and "Processed" shall have the meaning given to it in the UK GDPR;

"Protective Monitoring" means a set of business processes, used in order to oversee how systems are used to assure user accountability over their systems facilities.

"Quarterly Contract Review" Quarterly meetings between the Supplier and the Customer to manage and review the Supplier's performance under this Contract, as outlined in Part B of Schedule 3 (Service Levels & Service Credits).

**"Security Working Group" (SWG)** means the working group which meets to ensure a regular review of security matters concerning the test division between key stakeholders.

"Service Credits" means the service credits issued by the Supplier to Customer for failure to meet the Service Levels as set out at Schedule 3 (Service Levels & Service Credits);

"Service Levels" means the standards of performance to be met by the Supplier in providing the Support Services, details of which are set out at Schedule 3 (Service Levels & Service Credits) as amended from time to time in accordance with this Agreement;

"Service Minutes" means the total number of minutes for the month in question;

"Service Period" means a calendar month.

**"Service Recovery Plan"** means a written plan from the Supplier providing details of service improvements or rectifications that will return the service to performance levels as included within the Agreement, providing timelines for the rectification process;

"Services" means the:

- (a) Support Services; and
- (b) any other services provided or to be provided by the Supplier to Customer under this Agreement;

"Services Materials" means any materials, documents, processes and procedures, manuals, interfaces, including any know-how embedded in or which are an integral part of such materials, provided or made available by the Supplier (or any of their agents or sub-contractors) to the Customer under this Agreement

**"Software"** means the Supplier's standard software products as listed in Schedule 1 (Specification) as enhanced, modified, customised, configured or updated from time to time pursuant to this Agreement;

**"Software Licence Terms"** means the terms on which Customer and Customer Affiliates may use the Software under this Agreement as set out in Clause 9;

**"Software Updates"** means all releases, versions, bug fixes, upgrades of the Software that correct faults, add functionality or otherwise amend or upgrade the Software;

**"Software Warranty Period"** means the period of the Initial Period and any extension of this Agreement;

"Specification" means the applicable specification set out in Schedule 1 (Specification);

**"Supplier Contract Manager"** means or such other person notified in writing by the Supplier to Customer;

"Support Services" means the support services to be provided by the Supplier in accordance with Schedule 2 (Support Services);

"Third Party" means a person or entity other than the Parties; and

**"UK GDPR"** the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by Schedule 1

to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

- 1.2. The headings to clauses, appendices and schedules are inserted for convenience only and shall not affect the interpretation or construction of this Agreement.
- 1.3. Words expressed in the singular shall include the plural and vice versa. Words referring to a particular gender include every gender. References to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership, joint venture, government, state or agency of state.
- 1.4. The words and phrases "other", "including" and "in particular" shall not limit the generality of any preceding words or be construed as being limited to the same class as any preceding words where a wider construction is possible.
- 1.5. References to any statute, statutory provision, enactment, order, regulation or other similar instrument shall include:
  - (a) any subordinate legislation made under it;
  - (b) any provision which it has modified or re-enacted (whether with or without modification); and
  - (c) any provision which subsequently supersedes it or re-enacts it (whether with or without modification) whether made before or after the date of this Agreement.
- 1.6. All references in this Agreement to Clauses, Schedules and Appendices are to the clauses, schedules and appendices to this Agreement unless otherwise stated.
- 1.7. In the case of conflict or ambiguity then the provisions of:
  - (a) Clauses 1 to 28 of this Agreement shall prevail over the Schedules and Appendices; and
  - (b) the Schedules shall prevail over the Appendices.
- 1.8. This Agreement is entered into in the English language and all:
  - (a) amendments to this Agreement, all correspondence between the Parties concerning or relating to this Agreement; and
  - (b) notices given and all documentation to be delivered by either Party to the other pursuant to this Agreement in whatever form,

shall be in the English language. The English language version of this Agreement shall, if there is any conflict or ambiguity, take priority over any translated version.

## 2 <u>Commencement and Duration</u>

- 2.1. This Agreement shall (subject to the provisions for earlier termination in this Agreement, including Customer's rights to terminate in Clause 18) be deemed to have commenced on the Commencement Date and shall expire on 14<sup>th</sup> February 2022 ("Initial Period") unless it is extended in accordance with Clause 2.2.
- 2.2. Prior to expiry of the Initial Period the Customer may, upon at least three (3) months' prior notice in writing to the Supplier, and in its absolute discretion extend the duration of the Agreement by a period of up to 24 months (commencing on 15 February 2022) (the "**Extension Period**"). The terms and conditions of the Agreement shall apply throughout any such Extension Period.
- 2.3. From the Commencement Date, the previous rights the Customer had to use software equivalent to the Software under an agreement dated 22 December 2020 between (1) the Customer; and (2) LGC Genomics Limited have terminated and have been replaced by this Agreement.

### 3 Software and Services to be provided by the Supplier

<u>General</u>

- 3.1. The Supplier agrees to:
  - (a) grant to Customer a licence to use the Software on the Software Licence Terms; and
  - (b) deliver the Documentation to Customer as defined in Schedule 1 (Specification).

# Support Services

- 3.2. The Supplier hereby agrees to provide the Support Services in accordance with the Service Levels, commencing on the date set out in Schedule 2 (Support Services).
- 3.3. The Supplier shall make available to Customer, at no cost to Customer:
  - (a) Software Updates; and
  - (b) any new software product that replaces the Software to the extent that it includes a substantial portion of the functionality and/or features contained in the Software.

### 4 General Obligations of the Supplier

- 4.1. The Supplier undertakes:
  - (a) to perform all the Services:
    - (i) in a good and workmanlike manner;
    - (ii) in accordance with Good Industry Practice; and
    - (iii) in accordance with the provisions of this Agreement, including specifically the Service Levels;
  - (b) to provide the Services efficiently with the optimum use of all resources so as to provide the Services at the lowest reasonably obtainable overall cost and to actively seek ways of reducing costs;
  - (c) not to introduce any Disabling Device onto any Customer computer, server, mainframe or computer system. At no cost or expense to Customer, and without adversely impacting the Services, the Supplier shall reduce and/or eliminate the effects of any Disabling Device introduced by Supplier including by restoring and/or bearing the cost of re-creating and reinputting any lost data and/or software programming;
  - (d) not to disrupt the business or activities of and/or services provided by Customer;
  - (e) not to (and to procure that its personnel, agents, employees and sub-contractors shall not) through any act or omission cause Customer to infringe the terms of any licence or other agreement relating to the use, maintenance or support of the Software;
  - (f) to deliver the Documentation to Customer;
  - (g) to comply strictly with all legal requirements and Applicable Laws whilst performing its obligations under this Agreement; and
  - (h) to comply with the Escrow Agreement

### 5 <u>Undertakings and Representations</u>

- 5.1. The Supplier undertakes and represents that the Software shall be free from all Defects during the Software Warranty Period.
- 5.2. When notifying a Defect, Customer shall (so far as it is able) provide the Supplier with a documented example of such Defect.

- 5.3. The Supplier further undertakes and represents that:
  - (a) it owns all of the Intellectual Property Rights in the Software and has full capacity and all necessary licences, permits and consents to enter into and to perform this Agreement;
  - (b) this Agreement is executed by a duly Authorised Representative of the Supplier;
  - (c) neither it nor any of its officers, employees, agents, sub-contractors or any person acting on its behalf has offered, given or agreed to give any person any inducement or reward (or anything which might be considered an inducement or reward) in connection with Customer entering into this Agreement;
  - (d) it has the right to market, support, develop and supply to Customer the Software;
  - (e) the Documentation shall provide all necessary and adequate instructions to enable Customer's reasonably competent computer operators to make full and proper use of the Software and to facilitate the support, modification, and/or enhancement of the same by reasonably competent computer programmers;
  - (f) neither the Software nor the Services infringe nor will use of the same by Customer or its agents in accordance with this Agreement cause Customer to infringe any Third Party's Intellectual Property Rights; and
- 5.4. Except as expressly stated in this Agreement Customer makes no warranty, guarantee or commitment as to the term or length of relationship or amount of quantity (whether in units or monetary terms or service volumes) which Customer shall purchase or procure from the Supplier.

### 6 <u>Change Control Procedure</u>

- 6.1. For the purposes of this Agreement a "Change Request" is:
  - (a) a request to amend this Agreement, the Software or the Services;
  - (b) any matter which causes or is likely to cause Customer to incur additional costs or charges; or
  - (c) a change to any Service Levels except to the extent of any changes expressly permitted to be made unilaterally by Customer under this Agreement.
- 6.2. No Change Request shall be binding on the Parties unless the requirements of the Change Control Procedure have been satisfied and a Change Request form is signed by the Authorised Representatives of both Parties to signify their approval to the change.
- 6.3. Until such time as a Change Request is formally agreed to by both Parties, the Parties shall continue to perform their respective obligations without taking account of the Change Request.

- 6.4. Change Requests may be originated either by Customer or by the Supplier or may be originated by the Parties jointly. In the case of any Change Request, the Supplier shall within ten (10) Business Days either supply to Customer:
  - (a) full details (the **"Report"**) of all consequential changes which shall be required to:
    - (i) this Agreement;
    - (ii) the Service Levels; or
    - (iii) the payments due from Customer pursuant to this Agreement and all other effects of the proposed change; or
  - (b) written confirmation that there shall be no such consequential changes or effects.
- 6.5. In the event the Supplier gives notice to Customer within five (5) Business Days of receipt of a Change Request that it cannot provide the Report required by Clause 6.4 above within such ten (10) Business Day period, the Parties shall agree a suitable period within which the Supplier shall be required to provide these details. If the Parties are unable to agree such extension to the time-table within five (5) Business Days of receipt by Customer of such notice from the Supplier, the matter shall be referred for determination in accordance with the Dispute Resolution Procedure in Clause 26.
- 6.6. Customer shall use all reasonable endeavours to notify the Supplier that the Report is accepted or rejected by Customer within ten (10) Business Days of receipt of the Report by Customer. Customer reserves the right to refuse a Change Request originated by the Supplier entirely or to accept it but to specify a particular technical solution.
- 6.7. If a dispute arises as to whether any requirement of Customer or the Supplier is a Change Request the matter shall be dealt with in accordance with the Dispute Resolution Procedure in Clause 26.
- 6.8. On signature by both Parties of a Change Request form, this Agreement shall be deemed amended in accordance with the provisions of that Change Request form.

# 7 <u>Price & Payment</u>

- 7.1. Customer shall:
  - (a) pay the Supplier the Charges in accordance with this Agreement, subject to the Supplier issuing invoices to Customer in accordance with Schedule 4 (Charges); and
  - (b) not be liable to pay any amounts to the Supplier for the Services or Software under this Agreement unless the Charges for such Services or Software are expressly set out in this Agreement.

- 7.2. The Charges shall not be changed without the prior written consent of Customer (in its absolute discretion), unless expressly stated otherwise in Schedule 4 (Charges).
- 7.3. Unless stated otherwise in Schedule 4 (Charges), Customer shall pay the Charges in arrears within thirty (30) days from the end of the month in which Customer receives a valid and accurate invoice on which is stated a valid Customer purchase order number.
- 7.4. All sums to be paid under this Agreement shall be in pounds sterling and payment shall be in Pounds Sterling by electronic transfer to the bank account nominated by the Supplier from time to time, with any applicable charges on such payments being at the Supplier's sole cost and expense.
- 7.5. All sums payable under this Agreement are exclusive of VAT or any other applicable tax or duty which shall be payable at the rate and in the manner prevailing at the relevant tax point subject to the delivery of a valid VAT invoice.
- 7.6. If either Party fails to pay any amount due under this Agreement, the other Party is entitled (but is not obliged) to charge interest on the overdue amount, from the due date up to the date of actual payment, after as well as before judgement, accruing on a daily basis, at the rate of 2% per annum above the base rate for the time being of Barclays Bank plc.
- 7.7. If Customer has a bona fide dispute in respect of the whole or any part of any invoice then Customer shall notify the Supplier of the nature of such dispute in writing within thirty (30) days of receipt of the invoice giving all relevant details. If Customer notifies the Supplier in writing that it disputes the whole or any part of sums payable under any invoice in accordance with this Clause 7.7, Customer shall be entitled to withhold payment of the amount in dispute, but shall pay the undisputed part in accordance with this Agreement. The Parties shall cooperate in good faith to resolve the dispute over the invoice as amicably and promptly as possible. On settlement of any dispute Customer shall make the appropriate payment in accordance with this Agreement and with respect to any such settled amount any agreed period within which payments are due to be made shall commence on the date on which the dispute is resolved.
- 7.8. If any sums are due to Customer from the Supplier, then Customer shall be entitled to exercise the right to set-off such sums against any payments due to the Supplier from Customer under or in relation to this Agreement or any other agreement. The Supplier shall not be entitled to apply any amount due to Customer under this Agreement in or towards payment of any sum owing by Customer to the Supplier in relation to any matter whatsoever.

### 8 <u>Service Credits</u>

8.1. Pursuant to Clause <u>4.1(a)</u>4.1.(a), the Supplier shall perform the Support Services in accordance with the Service Levels so that Service Credits do not accrue.

- 8.2. At the end of each month, the Supplier shall provide Customer with a report setting out the Supplier's performance against the Service Levels in the immediately preceding month (the "**Preceding Month**") where the Supplier has failed to attain any Service Level, the Supplier shall provide Customer with the applicable Service Credit expressed as a percentage of the Charges levied in respect of the Preceding Month, such percentage to be calculated in the manner set out in Schedule 3 (Service Levels & Service Credits).
- 8.3. Customer's right to such Service Credits shall be in addition to, and not in substitution for, any other rights arising from the Supplier's failure to provide the Support Services in accordance with the terms of this Agreement.
- 8.4. Service Credits shall not be the sole and exclusive remedy of Customer with respect to the failure by the Supplier to meet the Service Levels to which the Service Credits relate and shall not limit any other rights or remedies Customer may have including termination and/or the right to claim damages.

### 9 Intellectual Property Rights

#### <u>Software</u>

- 9.1. The Supplier:
  - (a) shall retain all Intellectual Property Rights in the Software; and
  - (b) grants to Customer and the Customer Affiliates a right to use the Software in accordance with the Software Licence Terms.

#### Software Licence Terms

- 9.2. The Supplier grants to Customer a perpetual non-exclusive, irrevocable, royalty free licence to use the Software in Object Code form and the Documentation in relation to Customer's business. Customer may:
  - (a) permit any entities who are Customer Affiliates to access and/or use the Software on the terms set out in this Clause 9 for so long as they are a Customer Affiliate; and
  - (b) permit Third Party service providers to Customer and the Customer Affiliates to use, host and/or access the Software for the sole purpose of providing services to Customer and the Customer Affiliates (including software maintenance and support for the Software); and
  - (c) either:
    - sub-licence the use of the Software to (i) any Customer Affiliates for use in their businesses; or (ii) Laboratory Operators, on the same terms of this licence; or

- (ii) make copies of the Software and sub-licence such copies to (i) any Customer
   Affiliates for use in their businesses; or (ii) Laboratory Operators; and
- (d) install the Software in multiple environments, including Third Party locations and disaster recovery sites.
- 9.3. Except as stated in Clause 9.4 below, Customer has no right to assign the benefit of this licence without the prior written consent of the Supplier which shall not be unreasonably withheld or delayed.
- 9.4. Customer shall be permitted to assign the benefit of this licence as a whole to any Customer Affiliate or to an entity acquiring (in whole or part) Customer or its customer base or to a Third Party but only for use in the connection with the provision of services to Customer or a Customer Affiliate.
- 9.5. Except as stated in this Agreement, Customer has no right (and shall not permit any Third Party) to copy, adapt, reverse engineer, decompile, disassemble, modify, adapt or make error corrections to the Software in whole or in part except as permitted by law.
- 9.6. Customer may make such copies of the:
  - Software as are reasonably necessary for operational security and use. Customer shall ensure that all such copies bear the Supplier's proprietary notice; and
  - (b) Documentation as it requires to use the Software.
- 9.7. Any restrictions on Customer's use of the Software, for example volumes, number of End Users, servers or other metrics, shall be clearly set out in Schedule 1 (Specification) and the Charges associated with any increase and/or decrease in such metrics shall be set out in Schedule 4 (Charges). Customer may at any time increase or decrease such metrics by serving notice in writing on the Supplier. In the case of an increase once Customer has served notice on the Supplier and paid the increased Charges the relevant licence metrics shall automatically increase to the level specified in Customer's notice.
- 9.8. No additional terms other than as set out in this Agreement shall apply to Customer's access and use of the Software, Services and/or Documentation.

#### **Developed Work**

- 9.9. Any Intellectual Property Rights in any Developed Work, shall automatically vest in the Supplier, unless agreed otherwise in writing by the Parties.
- 9.10. The Supplier hereby grants to the Customer a royalty-free, non-exclusive licence to use and modify the Supplier Intellectual Property Rights, including if the Supplier retains it, Intellectual Property

Rights in the Developed Work (to the extent that it relates to the provision or receipt of the Services or use of the Software) during this Agreement and any exit period. The Customer shall have the right, following the expiry of any exit period, to use and (where agreed between the parties in writing) modify such Supplier Intellectual Property Rights as is agreed between the parties in writing. The Customer shall be entitled to sub-license the Supplier Intellectual Property Rights to the extent required to enable the Customer to receive the benefit of the Services and Software.

- 9.11. In case any Developed Work is identified as such by the Parties and Parties have agreed in writing to vest any Intellectual Property Rights in this Developed Work in the Customer, the Supplier shall assign with full title guarantee such rights to Customer. The Supplier shall execute such documents and take such steps as Customer may reasonably require to give Customer the full benefit of this Agreement.
- 9.12. In such case, the Supplier shall obtain waivers of all moral rights in any of the Developed Work to which any individual is now or may be at any future time entitled under Chapter IV of Part 1 of the Copyright Designs and Patents Act 1988 or any similar provisions of law in any jurisdiction.
- 9.13. Where any Developed Work produced by the Supplier pursuant to this Agreement and subsequently assigned to the Customer is subject to Pre-Existing Rights, the Supplier shall retain ownership of such Pre-Existing Rights, but grants to Customer a non-exclusive, irrevocable, perpetual, royalty-free licence to:
  - use such Pre-Existing Rights in any way whatsoever to facilitate and/or enable the use of the Developed Work; and
  - (b) to sub-licence such Pre-Existing Rights to Third Parties for the purpose set out in Clause 9.2 above.

#### <u>Marks</u>

- 9.14. All Marks are the property of Customer. Customer reserves all Intellectual Property Rights in relation to the use of such Marks.
- 9.15. The Supplier may not use any Marks or any similar Marks without the prior written permission of Customer.

#### <u>Indemnity</u>

9.16. The Supplier irrevocably and unconditionally agrees to indemnify Customer and/or its employees, sub-contractors and agents (who shall have no duty to mitigate their loss) in full and on demand and keep them so indemnified against all claims, demands, actions, proceedings and all direct and indirect damages, losses, costs and expenses (including without limitation legal and other professional advisers' fees, economic loss, loss of profit, future revenue, reputation, goodwill, anticipated savings)

and any consequential loss made against or incurred or suffered by any of them and whether wholly or in part resulting directly or indirectly from any claim that the operation, possession or use of the Software and/or Services or any constituent part by Customer or any Customer Affiliate, or its/their employees, sub-contractors or agents, infringes the Intellectual Property Rights of a Third Party whether or not such losses or the consequences of such matters were foreseeable at the date of this Agreement (an "**Intellectual Property Infringement**").

- 9.17. In the event of an Intellectual Property Infringement, Customer shall:
  - (a) give notice to the Supplier of any Intellectual Property Infringement as soon as reasonably practicable on becoming aware of the same;
  - (b) give the Supplier reasonable assistance in connection with the defence of any claim or action in respect of any Intellectual Property Infringement and not at any time admit liability or attempt to settle or compromise the said claim or action without prior consultation with the Supplier; and
  - (c) act (at the sole expense of the Supplier) in accordance with the reasonable wishes of the Supplier and give to the Supplier such assistance as it shall reasonably require in respect of the conduct of the said defence.
- 9.18. In the event of an Intellectual Property Infringement, the Supplier shall be entitled at its own expense and option either to:
  - (a) procure the right for Customer, Customer Affiliate or Laboratory Operators to continue using the Software and/or Services or the infringing part; or
  - (b) make such alterations, modifications or adjustments to the Software and/or Services or that infringing part so that it becomes non-infringing without incurring a material diminution in performance, capacity, resilience or functionality; or
  - (c) replace the Software and/or Services or that infringing part with non-infringing substitutes provided that such substitutes do not entail a material diminution in performance, capacity, resilience or functionality of the Software and/or Services (and the provisions of this indemnity shall apply equally to any such substitutes) reimbursing Customer or such Customer Affiliate or Laboratory Operators its reasonable costs associated with such substitution.

# 10 Data Protection

10.1. The Parties shall comply with Data Protection Laws throughout the term of this Agreement and shall if necessary enter into a separate data processing agreement.

#### 11 Employees

#### Supplier Personnel

- 11.1. The Supplier shall ensure that all its personnel engaged in the provision of Services under this Agreement shall be appropriately qualified and experienced.
- 11.2. Customer shall permit the Supplier's staff to gain access on reasonable prior notice at all reasonable times during normal office hours to any premises owned or occupied by Customer to enable the Supplier to carry out its obligations under this Agreement.
- 11.3. All staff provided by the Supplier for the purpose of carrying out its obligations under this Agreement shall at all times be and be deemed to be employees of the Supplier and not of Customer. The Supplier shall be responsible for paying all salaries, taxes, contributions and charges payable in respect of such employees and shall indemnify Customer against any claim by or in relation to such employees by virtue of or in connection with their contract of employment or provision of services by them.

### Key Personnel

- 11.4. The Supplier will ensure that each of the Key Personnel is committed to the provision of the Services, to the extent reasonably necessary to fulfil that individual's role in the provision of the Services during the term of this Agreement.
- 11.5. If it is necessary for the Supplier to remove any Key Personnel from their role, then the Supplier shall take reasonable steps to ensure that the new appointee is of sufficient qualification, experience and status within the Supplier's organisation to enable them properly to fulfil their responsibilities. Customer shall be entitled to object to any new appointee on reasonable grounds.
- 11.6. Customer reserves the right to attend interviews and approve personnel put forward by the Supplier as Key Personnel under this Agreement. Customer's approval of such personnel will not to be unreasonably withheld or delayed. If Customer does not approve such a member of personnel, it will provide the Supplier with specific reasons in writing for its decision at the time of notifying the Supplier of its decision.
- 11.7. Where a person is designated as Key Personnel, the Supplier shall ensure that there is a nominated and available deputy during any absence and equivalent replacement for consecutive periods of absence greater than five (5) Business Days.
- 11.8. The Supplier may only change the identity of the Key Personnel:
  - (a) for performance, disciplinary or career development reasons;

- (b) as a result of illness or resignation;
- (c) as a result of parental leave; or
- (d) where Customer consents to the change, which consent must not be unreasonably withheld or delayed.

### 12 Insurance

- 12.1. The Supplier shall at its own cost effect and keep in place with reputable insurers such insurance policies as are appropriate and adequate having regard to its obligations and liabilities under this Agreement. The Supplier shall throughout the term of this Agreement and for a period of six (6) years following termination or expiry of this Agreement have and maintain the following insurances with insurers of good repute at its own cost:
  - (a) employers' liability insurance for a minimum of £5,000,000 (five million pounds) per claim;
  - (b) public liability insurance (including product liability) for a minimum of £5,000,000 (five million pounds) for each occurrence; and
  - (c) professional indemnity insurance for a minimum of £5,000,000 (five million pounds) for each occurrence.
- 12.2. The Supplier shall on the written request of Customer from time to time provide Customer with reasonable details of the insurance policies maintained in force by the Supplier.
- 12.3. On the renewal of each insurance policy, the Supplier shall send a copy of the premium receipt to Customer when requested to do so in writing by Customer.
- 12.4. The Supplier shall do nothing to invalidate any of the insurance policies maintained in force in accordance with this Clause 12.

### 13 Liability and Indemnities

- 13.1. Nothing in this Agreement shall operate to exclude or limit a Party's liability for:
  - (a) death or personal injury arising from its negligence;
  - (b) fraudulent misrepresentation; or
  - (c) any other matter that cannot be limited or excluded by Applicable Law.
- 13.2. Nothing in this Agreement shall operate to exclude or limit the Supplier's liability to Customer under and/or in respect of any indemnity granted by the Supplier in this Agreement and/or any breach of

Clause 9 (Intellectual Property Rights), Clause 10 (Data Protection), Clause 14 (Compliance with Laws and Customer Policies), Clause 16 (Confidentiality) and Clause 24 (Bribery and Gifts).

- 13.3. Subject to Clauses 13.1 and 13.2, the aggregate liability of the Supplier arising under or in connection with this Agreement, whether in contract, tort or otherwise (including, in each case, negligence), shall not exceed the greater of:
  - (a) £5,000,000; or
  - (b) two hundred per cent (200%) of the total Charges which are payable (which shall include those Charges actually paid) by Customer to the Supplier under this Agreement.

Any amounts paid or payable by the Supplier from time to time in respect of liability referred to in Clauses 13.1 or 13.2 shall not count towards the liability cap in this Clause 13.3.

- 13.4. Subject to Clause 13.1, the aggregate liability of Customer arising under or in connection with this Agreement, whether in contract, tort or otherwise (including, in each case, negligence), shall not exceed the amount of the Charges payable by Customer to the Supplier under this Agreement. Any amounts paid or payable by Customer from time to time in respect of liability referred to in Clause 13.1 shall not count towards the liability cap in this Clause 13.4.
- 13.5. Other than in respect of matters or liabilities identified in Clauses 13.1 and 13.2, neither Party shall be liable to the other for any special, indirect or consequential losses or damages.

### 14 Compliance with Laws and Customer Policies

- 14.1. The Supplier shall:
  - (a) ensure that the Software and Services comply with all Applicable Laws; and
  - (b) comply with all Customer policies notified from time to time to the Supplier by Customer

### 15 <u>Contract Management and Audit</u>

- 15.1. The Supplier shall, and shall procure that any of its sub-contractors shall, during the term of this Agreement and for the period of six (6) years thereafter:
  - (a) maintain such records relating to the provision of the Services, the calculation of the Charges and/or the performance by the Supplier or sub-contractor of its obligations under this Agreement as required under any Applicable Laws, as is Good Industry Practice and as Customer may reasonably require in any form (including any electronic form) (the "Records");
  - (b) within two (2) Business Days of a request from Customer (or such other time frame as agreed

by the Parties) produce the Records for inspection by Customer or allow or procure for Customer and/or its Authorised Representatives access to any premises where any such Records are stored for the purposes of inspecting and/or taking copies of and extracts from such Records free of charge and for the purposes of carrying out an audit of the Supplier's or sub-contractor's compliance with this Agreement, including all activities of the Supplier or sub-contractor, the Charges and the performance, security and integrity of the Supplier or sub-contractor in fulfilling its obligations under this Agreement;

- (c) preserve the integrity of the Records in the possession or control of the Supplier or subcontractor and its personnel and all data which is used in, or generated as a result of, fulfilling its obligations under this Agreement and to prevent any corruption or loss of that data; and
- (d) provide any assistance reasonably requested by Customer in order to interpret or understand any of the Records.
- 15.2. At Customer's request, the Supplier shall attend review meetings with Customer concerning the results of any inspection of Records and shall make all reasonable changes required by, and take any other action necessitated by any inspection.
- 15.3. The Supplier shall, and shall procure that sub-contractors shall, provide Customer with such information as is reasonably necessary to enable Customer to determine the Supplier's or sub-contractor's compliance with the terms of this Agreement, and allow Customer, its employees or authorised agents access to such information to carry out appropriate inspections.
- 15.4. The Supplier shall, and shall procure that a sub-contractor shall, ensure that during any inspection of Records that Customer and/or the Customer Contract Manager receives all reasonable assistance and access to all relevant personnel, premises, systems, data, details of rebates and discounts received by the Supplier or sub-contractor and other information and records relating to this Agreement (whether manual or electronic) at the Supplier's or sub-contractor's premises, any premises where Records are kept and at all locations from which (in whole or in part) the Supplier or sub-contractor fulfils the terms of this Agreement.
- 15.5. If, following any inspection of Records, Customer can demonstrate that any amounts it has paid to the Supplier exceed the Charges which should have been payable as calculated in accordance with this Agreement, the Supplier shall forthwith pay or allow to Customer the amount of such over-payment and in the case of an over-payment exceeding 2% of the Charges which should have been payable as determined in the course of any such inspection and audit, the Supplier shall also (without prejudice to any other rights which Customer may have) reimburse Customer for the reasonable costs in conducting such inspection and audit together with interest, at the rate of 8% per annum above the official dealing rate from time to time on such over-payment being charged from the date on which it

was paid by Customer until the date on which Customer is reimbursed by the Supplier.

- 15.6. Without prejudice to Clauses 15.4 above and 15.7 below, in the event of an investigation into suspected fraudulent activity or other impropriety by the Supplier, any of its sub-contractors or any Third Party, Customer reserves for itself, any auditors or legal advisers of Customer and their respective authorised agents the right of immediate access to any other documents or materials relating to the Supplier's or sub-contractor's fulfilment of its obligations under this Agreement and the Supplier agrees, and shall procure that a sub-contractor agrees, to render all necessary assistance to the conduct of such investigation at all times during or after the term of this Agreement.
- 15.7. Customer shall have the right from time to time at its own cost to conduct an audit of the Supplier's or sub-contractor's operations and facilities and its quality, environmental and health and safety procedures and systems to ensure that the Supplier or sub-contractor has the appropriate facilities, procedures, systems and personnel appropriate to and as may be required for the Supplier or sub-contractor to fulfil its obligations under this Agreement, and otherwise in accordance with this Agreement and for that purpose shall be entitled to have access to the Supplier's premises and to any premises where the Supplier, its sub-contractors or agents fulfil the Supplier's obligations (part or all) under the Agreement during normal working hours on giving reasonable notice to the Supplier for that purpose.

#### 16 <u>Confidentiality</u>

- 16.1. Each Party shall keep and procure to be kept secret and confidential all Confidential Information belonging to the other Party disclosed or obtained as a result of the relationship of the Parties under this Agreement and shall not use nor disclose the same save for the purposes of the proper performance of this Agreement or with the prior written consent of the other Party. Where disclosure is made to any employee, consultant, sub-contractor, Third Party service provider or agent, it shall be done subject to obligations equivalent to those set out in this Agreement. Each Party shall use its best endeavours to procure that any such employee, consultant, sub-contractor or agent complies with such obligations. Each Party shall be responsible to the other Party in respect of any disclosure or use of such Confidential Information by a person to whom disclosure is made.
- 16.2. The obligations of confidentiality in this Clause 16 shall not extend to any information which the Party that wishes to disclose such information can show:
  - (a) is in, or has become part of, the public domain other than as a result of a breach of the obligations of confidentiality under this Agreement; or
  - (b) was in its written records prior to the 11 January 2021 and not subject to any confidentiality obligations; or

- (c) was independently disclosed to it by a Third Party entitled to disclose the same; or
- (d) is required to be disclosed under any Applicable Law, or by order of a court or governmental body or authority of competent jurisdiction or any recognised Stock Exchange, subject to the disclosing Party notifying and consulting with the other Party a reasonable time prior to such disclosure.
- 16.3. Nothing in this Clause 16 shall restrict, inhibit or affect any express rights that Customer has or is granted by the Supplier under this Agreement in respect of any Software.

### 17 Force Majeure

- 17.1. If either Party is affected by Force Majeure it shall immediately notify the other Party in writing of the matters constituting the Force Majeure and shall keep that Party fully informed of their continuance and of any relevant change of circumstances whilst such Force Majeure continues.
- 17.2. The Party affected by Force Majeure shall take all reasonable steps available to it to minimise the effects of Force Majeure on the performance of its obligations under this Agreement.
- 17.3. Save as provided in Clause 17.6 below, and subject to Clause 17.5 below, a Force Majeure shall not entitle either Party to terminate this Agreement and neither Party shall be in breach of this Agreement, or otherwise liable to the other, by reason of any delay in performance or non-performance of any of its obligations due to such Force Majeure and the date for performance of the obligations affected shall be deemed suspended only for a period equal to the delay caused by such Force Majeure.
- 17.4. The Party not claiming to be affected by Force Majeure is entitled to suspend its own performance of the Agreement including any obligation to make any payment under this Agreement while the Force Majeure continues without liability to the other and the Party affected by Force Majeure shall not be entitled to payment from the other Party in respect of extra costs and expenses incurred by virtue of the Force Majeure.
- 17.5. If the Party affected by Force Majeure fails to comply with its obligations under this Clause 17 then no relief for Force Majeure, including the provisions of Clause 17.3, shall be available to it and the obligations of each Party shall continue in force.
- 17.6. If the Force Majeure continues for longer than three (3) months the Party not suffering the Force Majeure event may, at any time whilst such Force Majeure continues, by notice in writing to the other terminate this Agreement on a date to be specified in that notice, which must not be less than fifteen (15) days or more than sixty (60) days after the date on which the notice is given.

#### 18 Termination

- 18.1. This Agreement may be terminated at any time by Customer after a duration of six (6) months from the Commencement Date without payment of compensation to the Supplier, by Customer giving to the Supplier not less than 1 month's prior written notice.
- 18.2. Either Party may immediately terminate this Agreement without payment of compensation by giving notice in writing to the other Party if any one or more of the following events happens:
  - (a) the other Party commits a material breach of any of its obligations under this Agreement;
  - (b) the other Party fails to remedy, where it is capable of remedy, or persists in any breach of any of its obligations under this Agreement after having been required in writing to remedy or desist from such breach within a period of thirty (30) days;
  - the other Party has any distress or execution levied or enforced on any of its assets which is not paid out within seven (7) days of it being levied;

(d)

- the other Party is deemed to be unable to pay its debts within the meaning of Section 123 of the Insolvency Act 1986; or
- the other Party calls a meeting for the purpose of passing a resolution to wind it up, or such a resolution is passed; or
- (iii) the other Party presents, or has presented, a petition for a winding up order; or
- (iv) an application to appoint an administrator is made in respect of the other Party or a notice of intention to appoint an administrator is filed in respect of the other Party; or
- (v) any other steps are taken by the other Party or any other person to appoint an administrator over the other Party; or
- (vi) the other Party has an administrator, administrative receiver, or receiver appointed over all or any part of its business, undertaking, property or assets; or
- (vii) the other Party takes any steps in connection with proposing a company voluntary arrangement or a company voluntary arrangement is passed in relation to it; or
- (viii) the other Party ceases, or appears in the reasonable opinion of the Party wishing to terminate likely or is threatening to cease to trade;

- (e) the other Party stops or suspends making payments (whether of principal or interest) with respect to all or any class of its debts or announces an intention to do so or the other Party suspends or ceases or threatens to suspend or cease to carry on its business;
- (f) a secured lender to the other Party takes any steps to obtain possession of the property on which it has security or otherwise to enforce its security; or
- (g) the other Party suffers or undergoes any procedure analogous to any of those specified in Clause <u>18.2(c)</u> to <u>18.2(f)</u> inclusive or any other procedure available in the country in which the other Party is constituted, established or domiciled against or to an insolvent debtor or available to the creditors of such a debtor.
- 18.3. In addition to its rights under Clauses 18.1 to 18.2 inclusive, Customer may immediately terminate the Agreement without payment of compensation to the Supplier if:
  - (a) the Supplier commits a Material Service Level Breach; or
  - (b) the Customer is not a beneficiary to the Bank Guarantee by the date set out in Clause 22.3
     (Bank Guarantee); or
  - (c) the Escrow Agreement is not executed by the date set out in Clause 22.4 (Escrow Agreement).
- 18.4. If the Supplier undergoes a Change of Control (or if it anticipates a Change of Control and, subject to Customer entering into a reasonable confidentiality agreement, the Supplier can disclose that potential Change of Control) the Supplier shall promptly (and within twenty (20) Business Days of that Change of Control) notify Customer in writing of that Change of Control, or potential Change of Control. The Parties shall discuss the effect of that Change of Control. If Customer has concerns about that Change of Control, it may terminate this Agreement immediately by written notice to the Supplier.

### 19 <u>Consequences of Termination</u>

- 19.1. On termination of this Agreement in whole or part for any reason whatsoever:
  - Subject to the Software Licence Terms, the relationship of the Parties shall cease and any rights or licences granted under or pursuant to this Agreement shall cease to have effect save as (and to the extent) expressly provided for in this Clause 19;
  - (b) any provision which expressly or by implication is intended to come into or remain in force on or after termination shall continue in full force and effect;
  - (c) each of the Parties shall immediately return to the other Party (or, if the other Party so

requests by notice in writing, destroy) all of the other Party's property in its possession at the date of termination, including all of its Confidential Information, together with all copies of such Confidential Information, and shall make no further use of such Confidential Information;

- (d) in the case of a partial termination of this Agreement and if there is no express term dealing with the reduction of the Charges then a fair and reasonable reduction shall be agreed and applied by the Parties.
- 19.2. A termination of this Agreement for reasons other than the release events as agreed between Parties in the Escrow Agreement, will ipso jure trigger a termination of the Escrow Agreement.

### 20 Assignment, Subcontracting and Third Party Rights

- 20.1. The Supplier shall not assign, delegate, transfer, charge or otherwise dispose of all or any of its rights and responsibilities under this Agreement.
- 20.2. The benefit of this Agreement shall be freely assignable by Customer and, in the event of any such assignment, all references in this Agreement to Customer shall be deemed to include its assigns.
- 20.3. Any Customer Affiliate and a successor may enforce any provision of the Agreement. Except for Customer Affiliates no person who is not a Party to this Agreement shall have the right (whether under the Contracts (Rights of Third Parties) Act 1999 or otherwise) to enforce any provision of this Agreement without the express prior agreement in writing of the Parties.
- 20.4. Where a person who is not a Party to this Agreement has a right to enforce any provision of this Agreement pursuant to Clause 20.3 above, the Parties to this Agreement may vary or terminate this Agreement by agreement between them without requiring the consent of that person.
- 20.5. The Supplier may not sub-contract any or all of its rights and obligations under this Agreement without the prior written consent of Customer (at its absolute discretion). The Customer hereby provides its written consent for the Supplier to sub-contract an element of Services or Software to each of the Approved Sub-Contractors in accordance with and as set out in Schedule 8 (Approved Sub-Contractors).
- 20.6. If Customer does permit the Supplier to sub-contract then:
  - (a) the Supplier shall:
    - (i) at all times remain liable to Customer for the performance of all of it duties and obligations under this Agreement (including any duties or obligations performed by the sub-contractor); and

- (ii) only be entitled to delegate or sub-contract as specified by Customer;
- (b) before entering into a sub-contract with the sub-contractor, the Supplier shall obtain
   Customer's approval of the form and content of that sub-contract;
- the Supplier shall require any such sub-contractor to be bound by all appropriate obligations corresponding to those placed on the Supplier by this Agreement;
- (d) at Customer's option, the Supplier shall require any such sub-contractor to covenant directly with Customer to observe and perform the obligations placed on the Supplier by this Agreement; and
- (e) the Supplier shall retain the right to terminate any agreement with any such sub-contractor in the event of any material breach by the sub-contractor of such an agreement, irrespective of whether such breach is remediable or not.

### 21 Entire Agreement

- 21.1. This Agreement and the documents expressly incorporated into this Agreement contains the entire agreement between the Parties in relation to its subject-matter and supersedes any prior written or oral agreements, representations or understandings between the Parties in relation to such subject matter.
- 21.2. The Supplier irrevocably and unconditionally waives any right it may have to claim damages for, and/or to rescind this Agreement because of breach of any warranty not contained in this Agreement, or any misrepresentation whether or not contained in this Agreement, unless such misrepresentation was made fraudulently.
- 21.3. The Parties acknowledge that this Agreement has not been entered into wholly or partly in reliance on, nor has either Party been given any warranty, statement, promise or representation by the other or on their behalf and other than as expressly set out in this Agreement.
- 21.4. To the extent that any warranties, statements, promises or representations have been given, each of the Parties irrevocably and unconditionally waives any right it may have to any claims, rights or remedies including any right to rescind this Agreement which it might otherwise have had in relation to them.
- 21.5. Nothing in this Clause 21 shall exclude liability for a fraudulent misrepresentation.

### 22 Financial standing of Supplier

- 22.1. The Supplier agrees to implement and maintain the following financial mitigations throughout the duration of the Agreement:
  - (a) Financial guarantee:
    - (i) ensure the Customer is a beneficiary to a guarantee from the Supplier's bank in accordance with Clause 22.3.
  - (b) Open book accounting:
    - The Supplier will maintain and retain Open Book Data throughout the term of the Agreement and for a period of 7 years thereafter; and
    - (ii) The Supplier must allow the Customer and its Audit Agents to access the Open Book Data throughout the duration of the Agreement and for a period of 7 years thereafter.
  - (c) Provision of management accounts:
    - (i) The Supplier will provide management accounts covering the period from 01.01.2021 to the termination or expiry of the Agreement. These will be provided on a month-by-month basis and updated with actuals and a revised forecast each month.
    - (ii) The management accounts will comprise the three standard statements (income statement, balance sheet and cashflow). Bank statements should also be made available, upon request, to confirm the cash position.
    - (iii) The management accounts provided by the Supplier to the Customer in execution of this obligation will be treated as Confidential Information and commercially sensitive information by the Parties and the Customer will limit access to the management accounts to its representatives on a need-to-know basis, provided that such representatives have undertaken the same confidentiality obligations.
    - (iv) If the Supplier's current ratio falls below 0.5x or its cash position falls below £125,000 then the Customer may:
      - (A) hold a meeting with the Supplier to review any effect on the continued delivery of the Services; and
      - (B) require the Supplier to produce a remediation plan which, when approved,

the Supplier will follow and provide regular updates to the Customer as to its progress.

- 22.2. The Customer can terminate the Agreement immediately and without payment of compensation if:
  - the Supplier fails to notify the Customer that its financial standing has fallen below the minimum acceptable cash and current ratio requirements set out in Clause <u>22.1(c)(iv)</u><u>22.1.(c)(iv)</u>;
  - (b) the Parties fail to agree the remediation plan referred to in Clause <u>22.1(c)(iv)(B)</u><u>22.1.(c)(iv)(B)</u>, which the Supplier will be given 10 days to prepare a draft working plan and, if rejected, 5 Business Days to rectify; and/or
  - (c) the Supplier fails to comply with the agreed remediation plan referred to in Clause 22.1(c)(iv)(B)22.1.(c)(iv)(B).

### Bank Guarantee

- 22.3. Supplier shall ensure that, on or before 30 June 2021, the Customer is a beneficiary to a guarantee from the Supplier's bank which shall:
  - (a) irrevocably and unconditionally guarantee a payment from the Supplier's bank to the Customer of up to one million pounds sterling (£1,000,000) ("Guarantee Payment") if cumulatively (1) the Supplier is in breach of this Agreement and (2) the Customer, notwithstanding the service of a notice notifying the Supplier of failure to remedy such breach, has not fully recovered any losses it has incurred as result of the Supplier's breach;
  - (b) include a term that the Guarantee Payment shall be recoverable by the Customer from the bank as a principal debt;
  - (c) be subject to English law and the exclusive jurisdiction of the English courts; and
  - (d) be substantially in the form set out in Schedule 6 (Bank Guarantee),

### (the "Bank Guarantee").

#### Escrow Agreement

- 22.4. The Parties shall ensure that, on or before 30 June 2021, they enter into a tri-partite escrow agreement with NCC Group Escrow Limited in substantially the form set out in Schedule 7 (Escrow) ("Escrow Agreement").
- 22.5. The Supplier shall in accordance with the Escrow Agreement, deposit the source code of any Supplier

Software and Software comprising the Services Materials in escrow.

- 22.6. The Supplier shall ensure that the deposited version of any source code is the current version and that the deposited version is kept up to date as new versions and Software updates are released.
- 22.7. Where the Supplier is unable to procure compliance with the provisions of clause 22.5 and clause 22.6 in respect of any third party Software, it shall provide the Customer with written evidence of its inability to comply with these provisions and shall agree with the Customer a suitable alternative to escrow that affords the Customer the nearest equivalent protection. The Supplier shall be excused from its obligations under this clause 22.7 only to the extent that the parties have agreed on a suitable alternative.
- 22.8. The Parties acknowledge and agree that the release of the materials pursuant to the Escrow Agreement shall be a last resort and shall only occur in the case that (cumulatively):
  - (a) The Supplier is in breach of this Agreement and has failed to remedy such breach having been notified by the Customer as set out in this Agreement; and
  - (b) Such breach by the Supplier cannot be remedied by execution of the Bank Guarantee.

### 23 <u>General</u>

#### **Relationship of the Parties**

23.1. Neither Party shall pledge the credit of the other Party nor represent itself as being the other Party nor an agent, partner, employee or representative of the other Party nor as having any power or authority to incur any obligation of any nature, express or implied, on behalf of the other Party. Nothing in this Agreement, and no action taken by the Parties pursuant to this Agreement, shall create, or be deemed to create, a partnership or joint venture or relationship of employer and employee or principal and agent between the Parties.

#### <u>Variation</u>

23.2. No purported alteration or variation of this Agreement shall be effective unless it is in writing, refers specifically to this Agreement and is signed by each of the Parties to this Agreement.

#### <u>Waiver</u>

23.3. The rights and remedies of either Party in respect of this Agreement shall not be diminished, waived or extinguished by the granting of any indulgence, forbearance or extension of time granted by such Party to the other nor by any failure of, or delay, by the said Party in ascertaining or exercising any such rights or remedies. Any waiver of any breach of this Agreement shall be in writing. The waiver by either Party of any breach of this Agreement shall not prevent the subsequent enforcement of that

provision and shall not be deemed to be a waiver of any subsequent breach of that or any other provision.

### Validity

23.4. If at any time any part of this Agreement (including any one or more of the clauses of this Agreement or any sub-clause or paragraph or any part of one or more of these clauses) is held to be or becomes void or otherwise unenforceable for any reason under any Applicable Law, the same shall be deemed omitted from this Agreement and the validity and/or enforceability of the remaining provisions of this Agreement shall not in any way be affected or impaired as a result of that omission.

#### **Counterparts**

23.5. This Agreement may be entered into in the form of two or more counterparts, each executed by one or more of the Parties (but taken together executed by all), and provided that all the Parties shall so enter into the Agreement, each of the executed counterparts, when duly exchanged or delivered, shall be deemed to be an original but, taken together, they shall constitute one instrument.

### 24 Bribery & Gifts

- 24.1. The Supplier warrants that is has never committed an offence under Sections 1, 2, 6 or 7 of the Bribery Act (a "**Bribery Offence**") or engaged in any conduct, whether by act or omission, before 1 July 2011, which if it had been made or carried out on or after 1 July 2011, would have constituted a Bribery Offence.
- 24.2. The Supplier agrees that in respect of all matters connected with or arising out of the Services and this Agreement, it:
  - (a) shall not, and will procure that its employees, sub-contractors and agents will not, commit any Bribery Offence or engage in any Foreign Bribery Conduct;
  - (b) has in place, and will maintain until termination or expiry of this Agreement, adequate procedures designed to prevent persons associated with the Supplier from bribing another person intending to obtain or retain business for the Supplier or to obtain or retain an advantage in the conduct of business for the Supplier (as envisaged under section 7(2) of the Bribery Act); and
  - (c) shall comply at all times with all obligations arising out of the Bribery Act.
- 24.3. The Supplier will not do or permit anything to be done through act or omission which would cause Customer, any employee, sub-contractor or agent of Customer or any Customer Affiliate to incur any liability under the Bribery Act or any other applicable legislation which prohibits any form of bribery

including, but not limited to, any legislation intended to implement the UN Convention Against Corruption.

- 24.4. The Supplier will not offer or give or agree to give any employee or agent of Customer or any Customer Affiliate any gift or consideration of any kind as an inducement or reward for doing or forbearing to do or for having done or forborne to do any act in relation to the obtaining or execution of this Agreement or any other agreement for Customer or any Customer Affiliate or for showing or forbearing to show favour or disfavour to any person in relation to this Agreement or any other agreement for Customer Affiliate.
- 24.5. Any breach of this Clause by the Supplier, its employees, agents or sub-contractors (whether with or without the knowledge of the Supplier) in relation to this Agreement or any other agreement for Customer or any Customer Affiliate, will be deemed a material breach of this Agreement, and, in addition, entitle Customer to recover from the Supplier the amount of any loss resulting from such material breach and to recover from the Supplier the amount or value of any such gift, consideration or commission.
- 24.6. The Supplier will notify Customer immediately if it becomes aware, or has reason to believe, that:
  - (a) it has breached any of its obligations arising out of this Clause 24; or
  - (b) any person or party directly or indirectly connected with the Services has committed any Bribery Offence, engaged in any Foreign Bribery Conduct or made, given, procured, received, or obtained any bribe (or attempted to do so).

#### 25 <u>Notices</u>

25.1. The address for notices to Customer is: 39 Victoria Street, Westminster, London, SW1H 0EU

Email:

With a copy to

25.2. The address for notices to the Supplier is:

UgenTec NV

att: Legal Department,

Kempische Steenweg 303/105, 3500 Hasselt, Belgium

Email:

25.3. Any notices sent under this Agreement must be in writing and may be served by personal delivery or by sending the notice by special delivery post or email at the address given above or at such other

address as the relevant Party may give for the purpose of service of notices under this Agreement and every such notice shall be deemed to have been served upon delivery if served by hand or at the expiration of two (2) Business Days after despatch of the same if delivered by special delivery post or if sent by email at ten hours (10:00) am local time of the recipient on the next Business Day following despatch.

25.4. To prove service of any notice it shall be sufficient to show in the case of a notice delivered by hand that the same was duly addressed and delivered by hand and in the case of a notice served by post that the same was duly addressed prepaid and posted in the manner set out above. In the case of a notice given by email, it shall be sufficient to show that it was despatched in a legible and complete form to the correct email address without any error message, provided that a confirmation copy of the transmission is sent to the recipient by first class post in the manner set out above. Failure to send a confirmation copy shall invalidate the service of notice by email.

### 26 Dispute Resolution Procedure

- 26.1. In the event of a material dispute between the Parties which has not been resolved in the normal course of business, either Party may call a meeting of the Parties by service of not less than ten (10) Business Days' written notice and each Party agrees to procure that the Customer Contract Manager and Supplier Contract Manager shall attend a meeting called in accordance with this Clause 26.1 with the aim of resolving the dispute.
- 26.2. Those attending the meeting pursuant to Clause 26.1 shall use all reasonable endeavours to resolve the dispute(s) arising out of this Agreement. If the meeting fails to resolve the dispute within ten (10) Business Days of its being referred to it, either Party by notice in writing may refer the dispute to an Executive Director (or their nominee) of Customer and a director of the Supplier, who shall co-operate in good faith to resolve the dispute as amicably as possible within fifteen (15) Business Days of the dispute being referred to them.
- 26.3. If the dispute between the Parties is not resolved having applied the process set out at Clauses 26.1 and 26.2, then the Parties may on the written request of both Parties (the "Dispute Resolution Request") agree in writing to enter into an alternative dispute resolution procedure (the "Dispute Resolution Procedure") with the assistance of a mediator agreed by the Parties or, in default of such agreement within fifteen (15) Business Days of receipt of the Dispute Resolution Request, appointed by the Centre for Effective Dispute Resolution, 70 Fleet Street, London EC4Y 1EU.
- 26.4. The Parties shall then submit to the supervision of the mediation by the Centre for Effective Dispute Resolution for the exchange of relevant information and for setting the date for negotiations to begin. The Parties shall bear their own legal costs of the Dispute Resolution Procedure, but the costs and expenses of mediation shall be borne by the Parties equally.

- 26.5. If the Parties agree to have recourse to the Dispute Resolution Procedure the same shall be binding on the Parties as to submission to the mediation but not as to its outcome. Accordingly all negotiations connected with the dispute shall be conducted in strict confidence and without prejudice to the rights of the Parties in any future legal proceedings. Except for any Party's right to seek interlocutory relief in the courts, no Party may commence other legal proceedings under the jurisdiction of the courts or any other form of arbitration until forty (40) Business Days after the appointment of a mediator.
- 26.6. If, with the assistance of the mediator, the Parties reach a settlement, such settlement shall be reduced to writing and, once signed by a duly Authorised Representative of each of the Parties, shall be and remain binding on the Parties.
- 26.7. Notwithstanding the provisions of this Clause 26 either Party may commence or take proceedings or seek remedies before the courts or any other competent authority for interim, interlocutory or injunctive remedies in relation to this Agreement.

# 27 <u>Law</u>

This Agreement and any issues, disputes or claims arising out of or in connection with it (whether contractual or non-contractual in nature such as claims in tort, from breach of statute or regulation or otherwise) shall be governed by, and construed in accordance with, English law.

### 28 Jurisdiction

Subject to first complying with the Dispute Resolution Procedure, all disputes or claims arising out of or relating to this Agreement shall be subject to the exclusive jurisdiction of the English Courts to which the Parties irrevocably submit.

IN WITNESS OF THE ABOVE the Parties have signed this Agreement on the date written at the head of this

SIGNED by	)
[insert name of signatory]	)
on behalf of	)
THE SECRETARY OF STATE FOR HEALTH	)
AND SOCIAL CARE	)

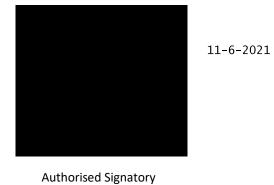


 SIGNED by
 )

 [insert name of signatory]
 )

 on behalf of
 )

 UGENTEC NV LIMITED
 )



### **Specification**

### 1. Background

1.1 The Supplier will licence FastFinder to the Customer for its continued use of the FastFinder software that conducts interpretative medical diagnostics of SARS-CoV-2 virus (Covid-19) tests, controls elements of workflow of the ePCR instrument and issue high volume results outputs from the ePCR instruments. The software licence will cover the use of the 10 ePCR machines already procured by the Customer and expected to be located at the UKBC Lighthouse lab and the new Megalabs, located in Leamington Spa, England and Glasgow, Scotland.

### 2. Expected outcomes

2.1 Fully functional FastFinder diagnostic software for interpretive medical diagnostics of Covid-19.

### 3. Supplier deliverables

- 3.1 Overview
  - (a) The Supplier will deliver the following:
    - Single licence for use across all DHSC designated sites for up to 50 concurrent End Users (85% doing results analysis 15% running diagnostics);
    - (ii) Maintenance and support of software;
    - (iii) Integration and deployment plan for rollout at additional sites;
    - (iv) Documentation requested for test assurance, such as plans and test reports for DR and BC, systems testing, security and performance testing; and
    - (v) Documentation requested for audit purposes, including SOPs on change and release management and software defect and risk management;

### 3.2 Professional services

(a) The Supplier will provide 24/7 support via its support desk. The Supplier will provide responses in line with the below response times:

Priority	Description	Category	Response Time
----------	-------------	----------	---------------

Low	Minimal business impact	Account creation, Not relevant for support	Two Business Days
Normal	Limited business impact	Complaint, feedback, technical support	One Business Day
High	Significant business impact	Complaint, feedback	One Business Day
Urgent	Critical business impact	Complaint	Within four (4) hours

- Minimal business impact: Items such as account creation and license request that do not impact the application. (Low priority).
- Limited business impact: Does not significantly impact operations, or a reasonable workaround is available. (Normal priority).
- (iii) Significant business impact: The application is usable but certain functions may be unavailable or severely limited. (High priority).
- (iv) Critical business impact: Unable to use the application. Requires immediate resolution. (Urgent priority).

### 3.3 Services to be provided

(a) Environments

 (i) FastFinder will be hosted on the Supplier's Microsoft Azure cloud service.
 Personal data concerning health will reside in Great Britain only. Other personal data (such as End User information) will reside in the European Union.

- (ii) Each site will have the following environments, hosted as separate instances from the other two sites: Testing (TEST), System Integration Testing 1 (SIT 1) and System Integration Testing 2 (SIT 2), User Acceptance Test (UAT), Non-functional Testing (NFT), Production (PROD) and Training (TRAIN).
- (b) Out of scope
  - (i) IT service provision for alternative or comparable diagnostic assay technologies to ePCR.

The Software solution shall, at a minimum, meet the Specification outlined in Appendix A of this Schedule 1.

Appendix A – Buyer Functional Requirements and Supplier Responses (As submitted in Supplier's proposal)

## MoSCoW weighting:

- Must have: (mandatory no workaround)
- Should have: difficult to workaround;
- Could have: short term workaround is satisfactory, or not mandatory at the moment; and
- Won't have: won't get now mandatory much later or wish list item

# Interface and LIMS entry requirements:

Requirements No	Main Area	Sub-Area	Description	MoScoW	Answer	Supplier Responses / Comments
GSF N0001	Functional	General	The system offers trained personnel the ability to easily access system data via an intuitive, user-friendly Windows-type graphical user interface (GUI) which permits the display of data from specimen points, projects, and user-defined queries, and can be configured to language, character set, and time zone needs.	Σ	Yes	
GSFN0002	Functional	General	The system allows authorized administrator to configure their GUI to a specific language, character set, and time zone.	Σ	Yes	
GSFN0003	Functional	General	The system permits remote access for End Users, system admins, and support agents.	Σ	Yes	
GSFN0004	Functional	General	The system allows for the use of navigation keys to freely move from field to field.	Σ	Yes	
GSFN0005	Functional	General	The system allows tabular data to be sorted and filtered.	Σ	Yes	

Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Σ	Σ	Σ	Σ	Σ	M	Σ	Σ	S	>
The system provides single data entry, automatically populates other data fields, and remembers pertinent and relevant data so it doesn't need to be re-entered, selected, or searched for.	The system can automate the search for and extraction of pertinent data. Super users can export that data to external applications for additional processing and calculation.	The system's numbering scheme allows for sub-numbering while maintaining parent-child relationships.	The system notifies End Users of events like the scheduling, receipt, and completion of tasks.	The system will track every transaction to include End User ID, date/time stamp and specific lab station	The system will allow the End User to track progress of samples to the analysis session, enabling the result file to map samples to related wells referenced by the outputting instruments	Transaction log/audit trail details must contain the End User ID of the person generating/entering the data or making the change to be captured and the Station ID at which the End User is working	Data must be entered into the system in a readable format and be unable to be deleted (unless the deletion is obvious and shown in the audit trail).	Data must be entered and accurately recorded by permanent means at the time the task is completed.	Data entered into the system must constitute the original data or must be verified and documented as a true copy.
General	General	General	General	General	Sample Prep Kingfisher Station	Data	Data	Data	Data
Functional	Functional	Functional	Functional	Functional	Functional	Data	Data	Data	Data
GSFN0007	GSFN0011	GSFN0015	GSFN0017	GSFN0022	GSFN0023	DA001	DA002	DA003	DA004

Ke		Yes	Yes	Yes	Maybe
Σ	Ś	≥	≥	Σ	3
Data must be accurately recorded and not be manipulated prior to entry into the system.	Raw Data: Data must be legible and accessible throughout the data lifecycle.	Raw Data: The system must permit the full reconstruction of the activities resulting in the generation of data.	MetaData: Metadata, including the attributing of data to an individual, must form an integral part of the original record.	Data Integrity: The accuracy, completeness, content and meaning of data must be retained throughout the data lifecycle (creation, storage, use, archival).	Primary Records: Where the same information is recorded concurrently by more than one system then the primary record must be defined.
Data	Data	Data	Data	Data	Data
Data	Data	Data	Data	Data	Data
DA005	DA006	DA007	DA008	DA009	DA010

Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3	Σ	3	3	3	Σ	3	≥
True Copies: Where copies of original data or records are retained in place of the original data or records there must be a documented process in place to verify and record the integrity of the copy, and that gives the ability to reconstruct records from a given raw data set.	The system supports a variety of test protocols, each capable of storing test comments, test required, and special information like assay or detector conditions or special objects associated with the test.	The system provides and enforces normal data range values for diagnostic tests.	The system includes default input values for diagnostic tests	The system provides for a single test code requiring multiple analyses as targets.	The system allows authorized End Users to make a test code inactive across one or more sites while retaining it for audit and reporting purposes.	The system limits test code authorization to only qualified personnel and maintains their certification(s) to run assigned tests.	The system allows End Users to specify a single-component, multi- component, or narrative text test or group of tests, which represent all tests required.
Data	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry
Data	Functional	Functional	Functional	Functional	Functional	Functional	Functional
DA011	ANDE0001	ANDE0002	ANDE0003	ANDE0004	ANDE0005	AN DE0006	ANDE0007

Yes	Yes	Yes	Not today	Yes	Yes	Yes	Yes	Yes	Yes
Σ	Σ	Σ	3	Σ	Σ	Σ	×	Σ	Σ
The system can effectively manage complex molecular testing protocols	The system distinguishes between routine and duplicate analysis.	The system provides an overview of all outstanding tests/analyses for better coordination of work schedules.	The system notifies analysts of applicable safety hazards associated with a sample, reagent, or test before testing begins.	The system electronically transfers an item during testing from one functional area to another.	The system's End User interface displays visual indicators such as status icons to indicate a sample's status in the workflow.	The system allows file transfer of data from instruments via files.	The system permits manual data entry into an electronic worksheet of test measurements and results.	The system allows incorrectly inputted data to be manually corrected.	The system prevents out-of-range and other critical results from being posted as final.
Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry
Functional	Functional	Functional	Functional	Functional	Functional	Functional	Functional	Functional	Functional
ANDE0008	ANDE0009	ANDE0010	ANDE0011	ANDE0012	ANDE0013	ANDE0014	ANDE0015	ANDE0016	ANDE0017

Yes	Yes	Yes	Yes	Not today	Not today	Yes	Yes
Μ	M	>	Σ	8	>	S	S
The system provides coloured visual indication of previously entered data as well as new data associated with a single sample when a result is entered, with the indicator changing colour if the value is out of specification.	The system allows automated or semi-automated data insertion.	The system stores non-narrative textual results in searchable fields.	The system updates sample/item status when tests are completed.	The system automatically reorders a test or orders additional tests if results don't meet lab-defined criteria, especially when the original sample is still available.	The system reads results from previously entered tests to calculate a final result and immediately displays the calculated result.	The system allows authorized End Users to review all analytical results - using business intelligence review tools	The system graphically displays the results of one or more tests in a graph (normalized or otherwise) for the purpose of visualizing data or searching for possible trends.
Analysis & Data Entry	Analysis & Data Entry	Analysis & Data Entry	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation
Functional	Functional	Functional	Functional	Functional	Functional	Functional	Functional
ANDE0022	ANDE0023	ANDE0024	PAVA0001	PAVA0002	PAVA0003	PAVA0004	PAVA0005

Yes	Yes	Yes	Yes	Not today	Yes	Yes	Yes
8	3	Σ	N	8	Σ	Σ	Σ
The system includes data mining tools for model learning, evaluation, and usage.	The system displays the standard operating procedure (SOP) associated with each test result to ensure proper techniques were used.	The system stores test-related analysis comments with the test.	The system provides auto-commenting for common laboratory result comments.	The system is capable of displaying entered order and test comments as an onscreen alert for testing and other personnel.	The system provides for high-volume multi-component transfers of test results, with the ability to automatically match samples to data files in either a backlog mode or a designated file mode, to parse the data, and to review and commit the sample data.	The system's results validation process accesses all information about a sample or group of samples, including comments or special information about the sample.	The system's results validation process checks each result against its individual sample location specifications (both warning and specification limits).
Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation
Functional	Functional	Functional	Functional	Functional	Functional	Functional	Functional
PAVA0006	PAVA0007	PAVA0008	PAVA0009	PAVA0010	PAVA0011	PAVA0012	PAVA0013

44

 Yes	Yes	Yes	Yes	Yes
Σ	Σ	×	Σ	Σ
The system supports validation at the analysis and sample level, while also prohibiting sample validation when analysis validation is incomplete.	The system uses a menu-driven process for results validation.	The system provides secure electronic peer review of results.	The system clearly differentiates released preliminary data from fully validated results.	The system validates/approves data prior to being moved to the main database.
 Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation
Functional	Functional	Functional	Functional	Functional
 PAVA0014	PAVA0015	PAVA0016	PAVA0017	PAVA0018

Yes	Yes	Yes	Yes	۶
Σ	3	≥	≥	≥
The system can hold all test results on a sample with multiple tests ordered on it until all work is completed and a final report is issued.	The system fully manages all aspects of laboratory quality control, including the reporting and charting of all quality control data captured in the lab.	The system distinguishes QA/QC duplicates from normal samples.	The system allows QA/QC tests to be easily created and associated with the primary analytical test.	The system allows manual entry of QA and QC data not captured as part of the system's regular processes.
Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation	Post Analysis & Validation
Functional	Functional	Functional	Functional	Functional
PAVA0019	PAVA0020	PAVA0021	PAVA0022	PAVA0023

Yes	Yes	Yes	Yes
 ≥	≥	S	≥
The system automatically flags out-of-range quality control limits.	The system checks data files for specification and corrects them for specific reporting and analyte limits and qualifiers like dilution factor, automatically assigning qualifiers based on project analyte limiting.	The system imports data from and exports data to Microsoft Word, Excel, and/or Access.	The system can interface with non-Microsoft programs.
 Post Analysis & Validation	Post Analysis & Validation		
Functional	Functional	External System Interfaces	External System Interfaces
 PAVA0024	PAVA0025	EXIF0001	EXIF0002

Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3	Σ	Σ	Σ	Σ	>	Σ	8	Σ
The system leverages the application programming interface (API) of other systems to establish integration between systems.	The system provides a real-time interface for viewing live and stored data transactions generated by interfaced instruments and systems.	The system directs output from ad-hoc queries to a computer file for subsequent analysis by other software.	The system supports the manual retransmission of data to interfaced systems.	The system includes a versatile report writer and forms generator that can generate reports from any data in tables.	The system allows the development of custom templates for different types of reports.	The system supports report queries by fields/keys, status, completion, or other variables.	The system uses Microsoft Office tools for formatting reports.	The system supports multiple web browsers for viewing online reports.
External System Interfaces	External System Interfaces	External System Interfaces	External System Interfaces	Reporting	Reporting	Reporting	Reporting	Reporting
EXIF0003	EXIF0004	EXIF0005	EXIF0006	REPT0001	REPT0002	REPT0003	REPT0004	REPT0005

Yes	Yes	Yes	Yes	Yes	Yes
3	8	*	≥	8	S
The system generates, stores, reproduces, and displays laboratory, statistical reports on demand, including narrative.	The system includes several standard reports and query routines to produce a backlog report.	The system indicates whether a report is preliminary, amended, corrected, or final while retaining revision history.	The system automatically generates individual and aggregate workload and productivity reports on all operational and administrative activities.	The system automatically generates and transmits exception trails and exception reports for all entered and/or stored out-of- specification data.	The system provides an ad-hoc reporting interface to report on End User-selected criteria.
Reporting	Reporting	Reporting	Reporting	Reporting	Reporting
REPT0006	REPT0007	REPT0008	REPT0009	REPT0010	REPT0011

### Results analysis:

Requirements No	Main Area Sub-Area	Sub-Area	Description	MoSCoW	Supplier Responses / Comments
RA001	Results		The system must track, display, analyse and provide a result status M (positive, negative, positive-limit-of-detection and void) each for individual sample.	Σ	
RA002	Results		The system must provide an audit trail of any changes to results data, time and date stamped.	Σ	
RA003	Results		The system must integrate with lab instruments, LIMS and other	Σ	

	Σ	Σ	×	Σ	Σ	Σ	Σ	Σ
systems as required.	The system must prevent out-of-range results from being posted as final.	The system must store test-related analysis comments with the test sample.	The system would provide auto-commenting for common laboratory result comments.	The system must supports validation at the analysis and sample level, while also prohibiting sample validation when analysis validation is incomplete.	The system must use a menu-driven process for results validation.	The system must provide for secure electronic peer review of results.	The system must clearly differentiate released preliminary data from fully validated results.	The system must validate/approve data prior to being moved to the main database
	Results	Results	Results	Results	Results	Results	Results	Results
	RA004	RA005	RA006	RA007	RA008	RA009	RA010	RA011

Σ	8	>	×
The system must automatically flag out-of-range quality control limits.	The system would automatically track data and transmit exception trails and exception reports for all entered and/or stored out-of-specification data.	The system would automatically generate and update control charts.	The system would generate QA/QC charts for all recovery, precision, and lab control specimens via a full statistics package, including Levy-Jennings plots and Westgard multi-rule.
Results	Results	Results	Results
RA012	RA013	RA014	RA015

## Non-functional requirements:

			:		
Requirements Main Area No	Main Area	Sub-Area	Description	MoSCoW	Kesponse
NFR01	Business		Backup and recovery;	N	
	Continuity &		a full backup and recovery service that covers all data and		
	Disaster Recovery		all service components in all of the environments, and		
			any backup or restore activity will not adversely affect the		
			performance or resilience of the 24 x 7 real time solution.		
NFR04	Business		Disaster recovery;	M	
	Continuity &		near instantaneous Recovery Time Objective (RTO), and		
	Disaster Recovery		Recovery Point Objective (RPO) as close to zero as possible		

N		Σ	3	×	3	3	3	×	S	S	A	S	S	S
Resilience to single- or multiple-point systems failure occurrences		The System is required to have detailed configuration/set up management documentation	All system data is required to be backed up regularly (backup trigger events/times to be configurable) to a 'Master Copy'	The 'master copy' of data is required to be stored in a separate location to the main system data copy	In the event that the data becomes corrupt, the system is required to provide the ability to restore data from the backup ('Master Copy')	In the event that the data becomes corrupt, the system is required to provide the ability to restore data from the backup ('Master Copy') within a minimum of 4 hours	The system is required to be designed to ensure that the personal data collected is able to be "deleted" in line with business retention policies	All system data is required to be stored within the UK	Any systems data that is stored is required to be done so in a secure repository only accessible by approved personnel	The system data must be transferred in a secure way using SFTP following ISO standard ISO 27001	Any personal data that is collected is required to be done so with consent from individuals in question clearly stating its use	DHSC will retain full ownership of the data and be able to pull data if a End User makes a data request in a timely manner but at the latest within 1 month	Personal data that is collected if required to be anonymized to protect privacy	The system is required to be able to notify on any data breach to allow this to be acted upon
	:	Contiguration manual	Data Backup	Data Backup	Data Restore	Data Restore	Data Retention	Data Storage	Data Storage	Data Transfer	GDPR	GDPR	GDPR	GDPR
Business Continuity & Disaster Recovery	:	Configuration/set up	Data Requirements	Data Requirements	Data Requirements	Data Requirements	Data Requirements	Data Requirements	Data Requirements	Data Requirements	Data Requirements	Data Requirements	Data Requirements	Data Requirements
NFR05		NFRU6	NFR09	NFR10	NFR11	NFR12	NFR13	NFR14	NFR15	NFR16	NFR17	NFR18	NFR19	NFR20

NFR21	General		Describe the output message types possible hI7, xml, fhir, W	
	Architecture and Interoperability		csv etc	
NFR24	Globalisation	Data Entry	Characters that are required to be allowed for data entry W	
		Characters	are required to be the same as those stated in ISO standard 27001	
NFR25	Globalisation	Data Entry	The system is required to show all labels in English, with the M	
		Language	End User being able to enter also in English	
NFR26	Globalisation	Internal Message Language	The system is required to display messages in English M	
NFR27	Globalisation	Multiple	The system is required to operate in the following M	
		countries	countries:	
			- England	
			- Wales - Scotland	
NFR28	Globalisation	Multiple	The system is required to enable the use of the M	
		Languages	following languages: - UK English	
NFR29	Globalisation	Time Stamp User Activity	All time-stamped activities are required to be captured in M	
		According to Time Zone		
NFR31	Hardware	Hardware	Any required Hardware shall be included in the price for the M	
			life of the service, additionally it must be included in the Asset management system including end of life details	
	-	_		
NFR32	Hosting &		Provide a Warranted Environment Specification for your S	
	Infrastructure		solution	
NFR33	Hosting & Infrastructure		Solution should be cloud agnostic	
NFR34	Implementation		The solution must be implemented with minimal disruption M to the current live operation. Describe how you will achieve	

×	>	8		8	≥ ≥	S	Σ
this and expected downtimes if any required The new solution must be implementable without significant impact to the existing operations	All external facing applications and websites must display proper convrights and trademarks	<ol> <li>Recovery Time Objective = Critical (24-48 hours) (Definition: The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity)</li> </ol>	<ol> <li>Recovery Point Objective = 0 hours (Definition-Recovery Point Objective (RPO) describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or "tolerance.")</li> </ol>	<ul> <li>System maintenance outages are required to be:</li> <li>planned/agreed in advance</li> <li>not in core hours (input hours)</li> <li>display a message to any applicable End User when occurring</li> </ul>	The system is required to have a reliability of 99.5% The system must continue to be available for 24 X 7 for 99.99% in any given month.	The Supplier must provide documentation on all elements	The Support system use. The Supplier of the Solution will publish training materials, including online training that will be available to all End Users of the Solution in time for UAT and thereafter keep it up to date. The Supplier of the Solution will, for the purposes of pricing, also provide super user training for 30 people and specific training materials to allow these trained
	Legal	IT Disaster Recovery / Service Continuity		Maintenance Window	Reliability System Availability		
Implementation	Legal Requirements	Operational		Operational	Operational Operational	People, Training &	Usability Usability
NFR36	NFR38	NFR39		NFR40	NFR41 NFR42	NFR44	NFR45

Ś	8	>	Σ	Σ				
Super users to train other End Users.The Supplier of the Solution will publish training materials,including online training that will be available to all EndUsers of the Solution in time for UAT and thereafter keep itup to date. The Supplier of the Solution will, for thepurposes of pricing, also provide super user training for 30people and specific training materials to allow these trained	Training for all elements of system use and necessary documentation.	Will state the level of training, required management of End User certifications, necessary knowledge transfer requirements	Solution should be designed in a way that enables it to scale to meet future volume and usage requirements of intended and anticipated test / software determination capacity	The projected volume of data for the next year is shown below, the system is required to at a minimum cater for these numbers:	<b>Overall:</b> The platform is required to support 3 Shifts of working patterns across 12 Lines and 2 Lab sites, therefore capacity requirements are as below:	Day 1 Feb 2021 - Line 1 Operational:	Minimum -Per Line Shift: 5,000 results analysed by LIMS (over 8 hours) -Size of Results File: 500 rows per result file CSV processed	Maximum -Per Line Shift: 30,000 results analysed by LIMS (over the period of a day) -Size of Results File: 500 rows per result file CSV processed
				Capacity				
People, Training & Usability	People, Training & Usability	People, Training & Usability	Performance and Capacity	Performance Requirements				
NFR46	NFR47	NFR48	NFR52	NFR53				

			All Lines Operational June 2021	
			Minimum -Per Line Shift: 30,000 results analysed by LIMS (over the period of a day) -Size of Results File: 500 rows per result file CSV processed	
			Maximum: -Per Line Shift: 60,000 results analysed by LIMS (over the period of a day) -Size of Results File: 1,000 rows per result file CSV processed	
NFR54	Performance Requirements	Performance monitoring	Performance and overall system monitoring tools are W required to be available to monitor performance, with any issues being managed as per the incident management requirement	
NFR55	Performance Requirements	Responsiveness	Onscreen usage response times are required to be between S 2-5 seconds, this is required to be the maximum time delay experienced by End Users	
NFR56	Performance Requirements	Scalability	To cater for increased use, the system is required to have M scalability to cater for Concurrent End Users: 50 (85% doing results analysis 15%	
			running diagnostics) Peak Load duration: 2 hours Endurance: 8 hours	
NFR57	Performance Requirements	End User population	The expected End User population is required to continue W to remain at 20 End Users	
NFR58	Performance Requirements	End User population	The system is required to cater for 20 End Users during the S seak usage time of 16:00-21:00 UK time	
NFR60	Production Support	Availability and critical hours of support	System support is required to be available 7 days a week Sam-9pm	
NFR61	Production	Change	Department will take the lead in managing the Change W	

	>	S	S	S	,	S		S		Σ		N		Σ	
Management process. Changes are required to be raised and completed a minimum of 90 calendar days prior to the requested implementation window unless it is an emergency change. Larger or more complex changes may require a longer notice period	<ul> <li>The following management of incidents process is required:</li> <li>Detection – Vendor will monitor with any alerts being escalated to Site Head to determine impact and severity</li> <li>Notification – Incidents found by End Users will be reported to Site Head via email or telephone. High severity incidents must be raised via telephone</li> <li>Remediation – Incidents will be analysed by Site Head and passed to the relevant development/BAU teams for resolution</li> </ul>	1st Level User Support is required to be supplied by Vendor 2nd and 3rd level Technical Support is required to be supplied by Vendor	State Cyber Assurance of Physical Security Systems (CAPSS) standard.	Access to databases must be restricted to authorized End	Users, computer processes or applications, and must be protected by authentication and authorization controls	All IDs and passwords for database access must conform to	the requirements outlined in the Identity and Access Control standard for password standards mentioned	Anonymous logon to databases is required to be prohibited		Database End Users are required to be prohibited from	granting access to anyone	Individuals must be uniquely authenticated to access any	database (enter if 2 factor authentications required)	Production databases must be physically or logically	separated from non-production databases (e.g. QA and Test)
management process	Incident management	Support Model	Hardware & software security	Database	Security	Database	Security	Database	Security	Database	Security	Database	Security	Database	Security
Support	Production Support	Production Support	Security	Security	Requirements	Security	Requirements	Security	Requirements	Security	Requirements	Security	Requirements	Security	Requirements
	NFR62	NFR63	NFR64	NFR70	l	NFR71		NFR72		NFR73		NFR74		NFR75	

>	×	Μ	Σ	3	Σ	Σ	Σ			Σ	Σ	3	3	Σ	N
Data is required to be held in multiple datacentres to allow for redundancy	The system and data must be hosted within the UK	Access to Password files is not allowed. Passwords can only be reset not viewed	All default passwords that are provided with the system are required to be changed prior to deployment	All passwords are required to be a minimum of 8 characters in length as per ISO standard ISO 27001	Before a password is changed, the current password is required to be entered unless reset by a security or system administrator	Controls are required to be in place to prohibit password reuse	For devices (workstations and terminals) and systems	(applications), inactive sessions must be shut down after 30 minutes of inactivity (please include devices utilised here if relevant also)	IDs are required to be disabled (made unusable) with a permanent lockout after a maximum of three (3) consecutive failed logon attempts	It is required that the system has protection from unauthorized access by any utility, operating system software and malicious software that are capable of overriding or bypassing system or application controls (enter current utilised software etc if known)	Locked accounts are required to remain in a locked status until manually unlocked by an administrator	Passwords are required to be changed at an interval not to exceed 30 days as per ISO standard ISO 27001	Passwords are required to be communicated in a secure manner according to ISO standard ISO 27001	Passwords are required to be masked, suppressed, or otherwise obscured during entry and creation	Passwords are required to be stored on the computer
Hosting	Hosting	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and	Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and
Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security	Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security
NFR76	NFR77	NFR78	NFR79	NFR80	NFR81	NFR82	NFR83		NFR84	NFR85	NFR86	NFR87	NFR88	NFR89	NFR90

	Σ	Σ	Σ	3	Σ	Σ	Σ	Σ	>	Σ	≥
platform (server) that provides the greatest level of security	Passwords that are initially assigned or reset by a system or security administrator are required to be valid only for one- time use, the system must force the End User to change the password at first logon	The ability to define and manage system access permissions and roles is required for the system	The allocation and use of privileges must be restricted, controlled and logged (input access levels and what they can access if known)	The password is required to contain a combination of letters (both upper and lowercase), numbers and special characters (although case is not mandatory) with the appropriate characters not being allowed as per ISO standard ISO 27001	The system is required to be configured to prompt End Users to change their password when the password has expired	The system is required to have a secure self-service process for password resets	The system must log all End User activity, including the activity of individuals who have access to restricted datasets/files or administrative/privileged access in the application/database/operating system production environment (Please deleted whatever element is not required for the system in question)	The End User is required to be notified of the locked status when their account is locked	Upon any account creation it is required that End Users enter their email address if required twice to prevent inaccuracies	When a password is reset, a confirmation is required to be sent to the End User/consumer via the communication method supported by the system (e.g. email)	All types of Personal Information are required to be encrypted in any kind of storage as per ISO standard ISO
Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Identity and Access Control	Information Assets
Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements
	NFR91	NFR92	NFR93	NFR94	NFR95	NFR96	NFR97	NFR98	NFR99	NFR100	NFR101

	8	3	3	S	S	S	≥
27001	Audit trails are required to be provided with the following to facilitate the tracing of processing and the reconciliation of disrupted data: 1. Type of activity 2. What changed 3. Who made the change 4. When did the change occur	Error handling procedures during information origination are required to be in place and must: 1. Must detect irregularities 2. Must report irregularities (e.g. End User's inputs are validated)	Information classified Secret, Confidential or Public must be labelled. Information classified as Proprietary must be labelled if transmitted or transported outside the main environment. All labelling must adhere to ISO standard ISO 27001	System Information is required to not be shared with unauthorized individuals or entities	Default accounts included in packaged software applications are required to be renamed, disabled, or have default passwords changed. (Any pre-established accounts that come with the tool or application out-of-the-box.)	Default passwords for application or service IDs are required to be changed according to requirements specified in the Identity & Access Control requirements	Each logged security event is required to record the following: following: 1. Identity information associated with the originating End User (e.g. Standard Identification No, End User name, and/or system accounts) 2. System or information resource that was accessed in the event 3. Event ID or Error Code 4. Result of event or type of action (e.g. authorize, create,
	Information Assets	Information Assets	Information Assets	Information Assets	Information System Controls	Information System Controls	Information System Controls
	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements	Security Requirements
	NFR102	NFR103	NFR104	NFR105	NFR106	NFR107	NFR108

on) mputer dating a access	ing the	ading so 5 and ation to	ut to W Land W	۲ ۲ ۳	ts to S End User
read, update, delete and accept network connection) 5. Subsystems performing action (e.g. process or transaction name) 6. Date and time of event 7. Source and Target (IP address, MAC address, Computer Name) 8. Source port and Target port 9. Before and after values if the action involves updating a data element 10. Whether the action was allowed or denied by access control mechanism	The system is required to encrypt authentication credentials in any transmission and storage following the ISO standard ISO 27001	The system is required to execute proper error handling so that: 1. Errors must not provide detailed system information to the End User 2. Errors will not deny service to the End User 3. Errors will not impair security mechanisms 4. Errors will not crash the system	The system is required to validate all End User input to ensure the types of input are legitimate and follow expected lengths and formats where validation occurs When authentication attempts fail, error messages are required to not indicate which part(s) of the credentials were invalid	Security event logs are required to be protected from: 1. Unauthorized access 2. Unauthorized modification 3. Unauthorized deletion	The system is required to provide a series of reports to comply with audit and legislative requirements on End User access: 1. Logged End User details report
	Information System Controls	Information System Controls	Information System Controls Information System Controls	Information System Controls	End User access
	Security Requirements	Security Requirements	Security Requirements Security Requirements	Security Requirements	Security Requirements
	NFR109	NFR110	NFR111 NFR112	NFR113	NFR114

	3	≥	S	8	≥	Σ	Σ	Σ	Σ
<ol> <li>End User deletion details report</li> <li>Password change details report</li> <li>End User access details report</li> <li>Function access details report</li> <li>Invalid access details report</li> <li>Audit trail report</li> </ol>	Availability; minimum of 99.99% availability will require no scheduled downtime (maintenance and associated releases will not incur service unavailability), and have automatic failover canability.	Maintain the batch operation of reports and extracts for backward compatibility purposes without adversely impacting the availability and performance for End Users of the real time functionality.	Please provide details on anticipated service scheduling	Proactive monitoring and reporting on the capacity of all key service components in all of the environments.	Standard online reports output within 9 seconds without affecting the performance or resilience of the solution.	Any required new software licenses must be agreed for the life of the service	Documentation and online/physical training is required to be available for the system	The system is required to have a comprehensive End User Guide detailing all functionality available to approved personnel only (add in any details if know who will be providing if out of box solution)	The solution must be able to integrate with the Customer as an IDP Provider (Active Directory Provider), either now or in the H1-2021 Product Roadmap
						Software Licensing	Training	End User manuals	Access and Identity Management
	Service	Service	Service	Service	Service	Software Licensing	Usability Requirements	Usability Requirements	Security
	NFR115	NFR118	NFR119	NFR120	NFR121	NFR122	NFR123	NFR124	NFR125

••
2
5
e U
+
Ś
~
S
3
2
2
3
~
2
9
8
2
2
2
2
>
-
-
5
2
3
CY .
_

Requirements No	Main Area	Sub-Area	Description	MoSCoW	Supplier Responses / Comments
QMS 001			The system shall display the most up to date version of the standard operating procedure (SOP) associated with each test result to ensure proper techniques were used. Are previous versions of the document required		
	General	SOP		Σ	
QM5002			The system fully manages aspects of laboratory quality control, including the reporting and charting of all quality control data captured in the lab.		
	General	Quality Control		8	
QM5003	General	Integration	The system can integrate with the LIMS as well other standard software i.e. MS Office	Σ	
QMS006			The system must provide workflow approval process to aid compliance		
	General	Workflows		N	

≥		>	2	Σ
The system shall manage end to end business processes such as risk & change management, accident, business continuity and incident management etc.	The system shall store validation reports and associated evidence to ensure to demonstrate that correct procedures have been followed. Any change to the process must be revalidated and evidence provided.		Indication of daily testing volume with implementation	timelines.
Process Management		Validation	Canacitu	Lapacity
General		General	Operational	Management
QMS007	QMS010		OPM001	

	8	M		×		N
Evidence of ISO13485 accreditation and details of scope, including if COVID-19 virology testing has been added to scope.		Quality Management system in place operating according to ISO13485		Evidence of regulatory arrangements in place e.g. CQC.	Business continuity plans in place.	
	Accreditation	Quality Management		Regulation	Business	Continuity
OPM001		OPM001	0PM001			

### Support Services

### 1. Service Level Targets

1.1 The table below sets out below service level targets upon which the Supplier's performance will be reviewed.

Priority	Description	Category	Response Time
Low	Minimal business impact	Account creation, Not relevant for support	Two Business Days
Normal	Limited business impact	Complaint, feedback, technical support	One Business Day
High	Significant business impact	Complaint, feedback	One Business Day
Urgent	Critical business impact	Complaint	Within four (4) hours

The target resolution time for any urgent issue is 4 hours, and performance is measured through the Monthly Uptime Percentage as set out in Schedule 3. For high impact issues, Customer and Supplier will agree on resolution times as validation of any change may be required.

This is also summarized in table below:

lssue Level	Cover	Target status update frequency	Target response time	Target resolution time
Critical Error	24/7	< 4 hours	4 hours	4 hours
High Impact Error	8:00am – 5pm UK	As required	One business day	As agreed between Supplier and Customer
Other Error	8:00am – 5pm UK	As required	Two business days	As agreed between Supplier and Customer

### 2. <u>Recovery Time Objective / Recovery Point Objective</u>

2.1 Table 1 below sets out the Supplier's commitment to recovery time and recovery point objectives. The Supplier's performance against such objectives will be reviewed in accordance with Part B of Schedule 3.

	Target
Recovery time objective	4 hours*

Recovery point objective 1 hour*
----------------------------------

Table 1

### Part A - Service Levels and Service Credits

### 1. Service Levels and Service Credits

- 1.1 Supplier performance will be discussed at the Quarterly Contract Review, but issues with performance may be escalated through the Supplier by the contract management team.
- 1.2 Where the Supplier fails to deliver the required performance, the Customer will raise concerns formally through the contract management team to the Supplier. The Supplier will be expected to produce a Service Recovery Plan of no more than two weeks which will then be instigated.
- 1.3 Where the Supplier fails to produce a Service Recovery Plan or fails to deliver agreed Service Recovery Plan to the required standard the Customer shall be entitled to terminate the Agreement in accordance with Clause <u>18.2(b)</u>.
- 1.4 Service Credits are payable by the Supplier where the Supplier falls below specified availability standards. Availability is determined by the monthly uptime percentage for the Service; the monthly uptime percentage is used to measure availability and is the percentage of time during which the Software is available for access and/or use by the Customer and the End Users (excluding scheduled Downtime), and shall be calculated and expressed over a period of one month by using the following formula:
  - (a) (Service Minutes-Downtime)/(Service Minutes) x 100,

### (the "Monthly Uptime Percentage").

The unavailability of a FastFinder plugin does not constitute unavailability of FastFinder.

- 1.5 Where Downtime is measured in minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month, excluding any downtime as a result of Customer's actions. The target Monthly Uptime Percentage is 99.99% and if the Monthly Uptime Percentage falls below 99.7% for any given month, the Supplier will be required to pay the following Service Credits:
  - (a) 99.99% to 99.7%: No Service Credits will be payable;
  - (b) <99.7%: For every 0.02% reduction in availability, the Supplier will pay a Service Credit of</li>
     1% of the monthly licence fee for the month in question, subject to a cap of 20% of the
     monthly licence fee for the month in question.

1.6 Should the Supplier reach the Service Credit cap of 20%, the Customer will be entitled to terminate the Agreement citing a Material Service Level Breach.

### Part B – Performance Monitoring

### 1. **Performance Monitoring**

- 1.1 Within twenty (20) working days of the Commencement Date the Supplier shall provide the Customer with details of how the processes in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as is reasonably possible.
- 1.2 The Supplier shall provide the Customer with the performance monitoring reports ("Performance Monitoring Reports") in accordance with this process and timescales agreed pursuant to paragraph 1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period:
  - (a) for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;
  - (b) a summary of all failures to achieve Service Levels that occurred during that Service Period;
  - (c) details of any Critical Service Level Failures;
  - (d) for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence; and
  - (e) such other details as the Customer may reasonably require from time to time.
- 1.3 The Parties shall attend meetings to discuss Performance Monitoring Reports on a Quarterly basis (the "Quarterly Contract Review Meeting"). The Quarterly Contract Review Meetings will be the forum for the review by the Supplier and the Customer of the Performance Monitoring Reports. Quarterly Contract Review shall:
  - take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Customer shall reasonably require;
  - (b) be attended by the Supplier's Authorised Representative and the Customer's AuthorisedRepresentative; and

- (c) be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Customer's Authorised Representative and any other recipients agreed at the relevant meeting.
- 1.4 The minutes of the preceding quarter's Quarterly Contract Review Meeting will be agreed and signed by both the Supplier's Authorised Representative and the Customer's Authorised Representative at each meeting.
- 1.5 The Supplier shall provide to the Customer such documentation as the Customer may reasonably require in order to verify the level of the performance by the Supplier for any specified Service Period.

### Security Undertakings

The Supplier will meet and maintain the following security undertakings for the Initial Period and any extension of this Agreement:

### 1. <u>Governance</u>

- 1.1 A security management system (the "**System**") including a plan must be developed and maintained, structured in accordance with ISO27001:2013, to cover the Information Assurance aspects throughout the life of the Agreement. This will include scope, statement of applicability, risk management plans, and other artefacts all of which must be agreed with the Customer.
- 1.2 There must be a named accountable person from the Supplier who is accountable for the provision of technical, personnel, process and physical security aspects for the scope of the Agreement, including but not limited to security clearances.
- 1.3 The Customer must have the ability to audit and assess security controls at any of the sites used for the purpose of meeting the Agreement.
- 1.4 Security must be embedded in all service management including but not limited to change management, incident management, and other service management artefacts aligned with ISO2000.
- 1.5 Development and test environments must have assured separation from the live/production systems, and must not use live / production information without prior written Customer approval.
- 1.6 The System must be configured in line with the law, regulations and the Customer's policies, standards and guidance including but not limited to malware policy, patching policy, password standard, information handling and security monitoring.
- 1.7 The System and locations must have auditable authorisation, authentication and access control based on least privilege, and aligned appropriate to the business requirement.
- 1.8 The System and processes must enforce separation of duties based upon the agreed risk assessment and management.
- 1.9 The System must be developed and reviewed against the best commercial practices, including security testing of the infrastructure and applications, in line with HMG standards and guidelines.
- 1.10 The System should notify End Users to read and accept the terms and conditions of service, annually.

### 2. Risk Assessment

- 2.1 The Supplier will undertake risk assessment of the whole system and supporting process in line with their Information Security Management System and the Customer's Standards and including when system changes are made. The Customer retains the rights to review the repeatable methodology used for risk assessment.
- 2.2 The Supplier must share with the Customer the outputs of the risk assessment, mitigation actions and any remaining remediation plans.
- 2.3 The Supplier must engage with the Customer with regards to managing all security-related risks to ensure they are within risk appetite / tolerances or there is a risk exception acceptance, in writing from the Customer, as a minimum through active attendance at the nominated Security Working Group.

### 3. Awareness & Training

3.1 It must be ensured that all staff and subcontractor's End Users and relevant employees are provided with appropriate security education, training and awareness, with this aspect being reviewed at least annually and whenever personnel roles change. Training shall include elements of physical, personnel and electronic security guidance.

### 4. <u>Personnel Security</u>

4.1 The Supplier must provide screening controls that conform to the Baseline Personal Security Standard (BPSS) for all staff and subcontractors who have any access to the system and information with regards to the System both logically and physically. There may be a requirement for high clearances based on the risk assessment and risk management.

### 5. Operational Security

- 5.1 The Supplier must have security operational awareness, detection, prevention, response and remediation processes / controls to effectively manage security incidents.
- 5.2 The Supplier must conduct vulnerability, security, penetration testing and address the findings or have the Customer accept in writing findings that will not be addressed.

### 6. Architectural Principles

- 6.1 The Supplier must ensure that the System and associated infrastructure is designed in a manner to ensure effective physical and logical separation, including but not limited to:
  - (a) Manufacturing and back office networks and services must not exist on the same subnet

(b) Operative and administrative activities must not be possible using the same accounts

### 7. <u>Protective Monitoring</u>

7.1 The Supplier must adopt the Customer's preferred Protective Monitoring capability or provide their own which is recognised as exceeding the former.

### **Charges**

### 1. Charges

1.1 The following Charges shall apply on a monthly basis:

Pricing component	Price excluding VAT, £	
Monthly licence fee	£	
Price per 100,000 tests	£	

- 1.2 In addition, the following volumes discounts will apply to the price per test:
  - (a) If volumes exceed the 'full' volume thresholds below, a discount of will be applied, if volumes exceed the 'reduced' volume thresholds below, a discount of will be applied. Discounts will apply at the end of every month depending on # of tests processed that month.
  - (b) If the total volume in the Initial Period of samples exceeds the total 'full' volume threshold or exceeds the total 'reduced' volume threshold, the discount of respectively will apply to all volumes including those volumes performed during individual months that did not cross the threshold. The final invoice will reflect these calculations if necessary.
- 1.3 The discount rate is based on the following volumes:

Date	Full volumes	Reduced volumes	
	# of tests po	# of tests per month	
Mar-21	N/A	N/A	
Apr-21	N/A	N/A	
May-21	22,000,000	6,500,000	
Jun-21	22,000,000	6,500,000	
Jul-21	22,000,000	6,500,000	
Aug-21	22,000,000	6,500,000	
Sep-21	22,000,000	6,500,000	
Oct-21	22,000,000	6,500,000	
Nov-21	22,000,000	6,500,000	
Dec-21	22,000,000	6,500,000	
Jan-22	22,000,000	6,500,000	
Feb-22	11,000,000	6,500,000	

Total	209,000,000	61,750,000
Volume discount applicable, %		

1.4 For example, the following discounts will apply in the month of April:

# of tests per month			
Apr-21	>22,000,000	> 6,500,000	<=6,500,000
Volume discount applicable, %			

1.5 For the avoidance of doubt, the Agreement price is not subject to any minimum or maximum test volumes and will not be subject to indexation adjustments during any extended term.

### 1.6 Any re-purposing of the software, will be subject to the below costs:

Grade description	Hourly Rate (£ excl. VAT)
Development services (such as assay plug-in development, dashboard development or any platform change requests)	£

Environments	Annual Fee per environment (£ excl. VAT)
Annual fee for installation, maintenance and hosting of additional environment (such as a separate test or UAT environment)	£

Bank Guarantee

### Escrow Agreement



### Approved Sub-Contractors

APPROVED SUB-CONTRACTOR Microsoft Microsoft Inc, One Microsoft Way, WA 98052-6399, Redmond, USA Registration: SEC CIK #0000789019	ELEMENT OF THE SERVICES OR SOFTWARE TO BE SUB- CONTRACTED TO THE APPROVED SUB-CONTRACTOR Hosting provider for the FastFinder platform
HubSpot HubSpot Inc. 25 First Street, 2nd Floor, MA 02141, Cambridge, USA Registration: SEC CIK #0001404655	Customer relationship management platform
ZenDesk Zendesk Inc, 989 Market St , CA 94103, San Francisco, USA Registration: SEC CIK #0001463172	Support management platform
Teamleader Teamleader NV, Dok Noord 3A/101, 9000, Gent, België Registration: BE 0899.623.035	Electronic resource planning platform

Atlassian	Project management and product
Atlassian Inc, 341 George Street, 2000, Sydney, NSW, Australia	development tool
Registration: SEC CIK #0001650372	
Registration Link: <u>https://sec.report/CIK/0001650372</u>	
Pendo	User analytics monitoring tool
Pendio.IO, Inc, 418 South Dawson Street Raleigh, NC 27601, USA	
Registration: SEC CIK #0001595931	
Registration link: https://sec.report/CIK/0001595931	