


ORDER FORM For the provision of IT SERVICES		 CITY OF LONDON
PURCHASE ORDER No.		
DATE:	9 DECEMBER 2021	

The Customer appoints the Service Provider to perform the Services subject to and in accordance with:

- the **Particulars** listed below;
- The **Standard Terms and Conditions for IT SERVICES** (the "**Standard Terms and Conditions**") comprising:
 - **Part A (General Terms and Conditions);**
 - **Part B (Support and Maintenance SLA);**
 - **Part C (Definitions);**
 - **Part D (Data Protection GDPR);**
 - **Part F (Tender Documents);**
 - **Part G (Change Control Form);**
 - **Part H (Certificate of Declaration);**
 - **Part I (Contacts List);**
 - **Part J (Special Terms and Conditions);**
 - **Part K (Service Recipient Agreement).**

all of which form part of this Order Form.

Ref.	PARTICULARS	
	Background to this Order:	The Customer conducted a PCR 2015 compliant, Open Procurement for the provision of the Police CyberAlarm services.
	Customer:	THE COMMON COUNCIL OF THE CITY OF LONDON (in its capacity as Police Authority for the City of London), whose principal address is at Guildhall, PO BOX 270, London EC2P 2EJ
	Service Provider:	Pervade Software Ltd, whose address is, Castle Court, Cardiff, CF11 9LJ; Company Number 0706728
	IT Services for:	The provision of the next iteration of the Police CyberAlarm, including additional functionality in respect of ingesting/enriching/categorising firewalls.

		<p>analysis and event reporting, and scanning of external IP/websites of member organisations, to provide enriched intelligence source for policing and other developments.</p> <p>Comprising of SaaS, Implementation, Hosting and Support and Maintenance – all as describe in Part F,1 and further in this agreement.</p>
PART A	STANDARD TERMS & CONDITIONS	
Clause 3.1	Commencement Date:	01 December 2021
Clause 3.1	Initial Term:	1 Year
Clause 3.2	Subsequent Term(s):	1 Year + 1 Year
Clause 9.1	Charges:	<p>Total Charges for the Initial Term: £359,340.59 exclusive of VAT;</p> <p>Total estimated charges for the Project, should targets be met and funding provided for optional extensions in year 2 and 3: £1,493,127.32;</p> <p>Detailed breakdown of the Charges are set out in Part F,2</p> <p>Monthly milestone payments will apply</p>
Clause 9.2	Retention:	None
Clause 16.1	Insurances required:	<ul style="list-style-type: none"> Professional Indemnity Insurance of s43(2) for each and every claim; Public Liability Insurance of s43(2) for each and every claim; Employer's Liability Insurance at an amount equal to or more than s43(2) as required by law; and, Cyber Security and Data Protection cover of s43(2)
Clause 17	Intellectual Property Rights Options	OPTION 2
Clause 41	Parent Company Guarantee:	No
	Customer's Contacts:	See Part I
	Service Provider's Contacts:	See Part I
PART B	SLA	

Para 2.1	Support Hours	Core Support Hours are: s43(2) Extended Support Hours are: s43(2) All times are London time
-----------------	----------------------	--

EXECUTION CLAUSE FOR CONTRACTS VALUED £250,000 AND ABOVE

IN WITNESS whereof this Order Form is prepared in duplicate and executed to take effect on the date first written

EXECUTED and DELIVERED as a DEED
by SERVICE PROVIDER
by means of these signatures:

s40(2)

Director

s40(2)

Director / Company Secretary

s40(2)

THE COMMON SEAL of the
The Mayor and Commonalty and Citizens
of the City of London
was hereunto affixed in the presence of:

s40(2)

Assistant City Solicitor

Authorised Signatory

Examined	NP	
Ctee/Court	DELEGATED COMMISSIONER	
Date	15.12.2020	
Passed for Sealing	NP	
Fund	CITY FUND	
Power	S111 LGA 1972	
Seal Follo No.	2021 / 773	





STANDARD TERMS AND CONDITIONS

FOR

IT SERVICES

PART A
GENERAL TERMS AND CONDITIONS

RECITALS

- (A) The Customer wishes to procure IT Services from the Service Provider following a tendering process.
- (B) The Service Provider having experience in providing the IT Services accepts the appointment on the terms and conditions of this Agreement.

NOW IT IS AGREED as follows:

1 Definitions and Interpretation

- 1.1 In this Agreement, unless the context otherwise requires, defined terms are described in **Part C (Definitions)**:
- 1.2 In this Agreement, unless the context otherwise requires:
 - 1.2.1 the singular includes the plural and vice versa;
 - 1.2.2 reference to a gender includes the other gender and the neuter;
 - 1.2.3 words importing persons include firms, companies and corporations and vice versa;
 - 1.2.4 any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment;
 - 1.2.5 references to numbered clauses, Parts and Schedules are references to the relevant clause, Part or Schedule to this Agreement;
 - 1.2.6 references in any Part or Schedule to numbered paragraphs relate to the numbered paragraphs of that Part or Schedule;
 - 1.2.7 any obligation on a party not to do or omit to do anything is to include an obligation not to allow that thing to be done or omitted to be done;
 - 1.2.8 a party who agrees to do something shall be deemed to fulfil that obligation if that party procures that it is done.
- 1.3 The headings in this Agreement are for ease of reference only and shall not affect its interpretation.
- 1.4 In case of conflict or ambiguity between the Standard Terms and Conditions and the Special Terms and Conditions contained in the Order Form, the Special Terms and Conditions shall take precedence.

2 Due Diligence

- 2.1 The Service Provider acknowledges that it:
 - 2.1.1 has made and shall make its own enquiries to satisfy itself as to the accuracy and adequacy of any information supplied to it by or on behalf of the Customer;
 - 2.1.2 has raised all relevant due diligence questions with the Customer before the

commencement date of this Agreement;

2.1.3 is confident it can fulfil its obligations according to these terms; and

2.1.4 has entered into this Agreement in reliance on its due diligence.

2.2 The Service Provider shall be deemed to have entered into this Agreement with full knowledge of the IT Services to be performed and the terms of this Agreement.

3 Duration

3.1 This Agreement shall start on the Commencement Date and, unless terminated earlier, shall continue until the end of the Initial Term.

3.2 Unless the Agreement is terminated at the end of the Initial Term, the Customer may extend the Agreement for a Subsequent Term (up to the maximum number of extension periods described in the Order Form) by notice in writing served prior to the expiry of the Initial Term or relevant Subsequent Term.

4 IT Services

4.1 The IT Services to be provided are described in **Part F (Tender Documents)**.

5 Implementation

5.1 The Service Provider shall deliver an outline Implementation Plan to the Customer within seven (7) days of the Commencement Date.

5.2 A detailed Implementation Plan shall be agreed with the Customer, within seven (7) days of delivery of the outline Implementation Plan, with sufficient detail as is necessary to manage the implementation of the IT Services effectively.

5.3 Once the detailed Implementation Plan has been agreed with the Customer; performance shall be measured against the detailed Implementation Plan.

5.4 The Service Provider shall report weekly on progress. If any issues are raised on the quality, the Deliverables or any other matter related to the work done within the weekly reporting period, the Service Provider shall have five (5) working days to respond to the issues and make any changes required.

6 Implementation Delays

Delays due to Service Provider

6.1 If at any time the Service Provider becomes aware that it shall not (or is unlikely to) achieve any Milestone by the Milestone Date it shall as soon as reasonably practicable (and not later than five (5) working days) notify the Customer in writing of the Delay, giving full details of:

6.1.1 the reasons for the Delay;

6.1.2 the consequences of the Delay and impact on other Milestones and Go-Live; and

6.1.3 a draft Correction Plan detailing the steps that the Service Provider proposes to take to achieve the Milestone.

6.2 The draft Correction Plan shall be submitted to the Customer for approval.

- 6.3 The Service Provider shall comply with the Correction Plan following its approval by the Customer.
- 6.4 The Customer may at its sole discretion (without waiving any rights in relation to other options) choose to:
- 6.4.1 issue a Conditional Milestone Achievement Certificate with an agreed Correction Plan; and/or
 - 6.4.2 refuse to issue a Conditional Milestone Achievement Certificate and escalate the matter in accordance with the Dispute Resolution Procedure, and if the matter cannot be resolved, exercise any right it may have under this Agreement or at law.
- 6.5 Where the Customer issues a Conditional Milestone Achievement Certificate, the Customer can choose to (but is not obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

Delays due to Customer Cause

- 6.6 If the Service Provider would have been able to achieve a Milestone by its Milestone Date but has failed to do so as a result of a Customer Cause, the Service Provider shall:
- 6.6.1 be allowed an extension of time equal to the Delay caused by the Customer Cause; and
 - 6.6.2 not be in breach of this Agreement as a result of the failure to achieve the relevant Milestone by its Milestone Date.
- 6.7 The Customer shall:
- 6.7.1 consider the duration of the Delay, the nature of the Customer Cause, the effect of the Delay on the Service Provider's ability to comply with the Implementation Plan;
 - 6.7.2 consult with the Service Provider in determining the effect of the Delay;
 - 6.7.3 fix a revised Milestone Date, and
 - 6.7.4 if appropriate, make a consequential revision to subsequent Milestones and/or Milestone Dates in the Implementation Plan.
- 6.8 The Customer shall, at its absolute discretion, determine in prior consultation with the Service Provider if a CCN is required to be issued in accordance with the requirements of clause 26.
- 6.9 The Service Provider shall, and shall procure each sub-contractor to, take and continue to take all reasonable steps to eliminate or mitigate any losses and/or expenses that it incurs as a result of a Customer Cause.

Delays not due to one party alone

- 6.10 Where a Delay is attributable in part to the Service Provider and in part to a Customer Cause, the parties shall negotiate in good faith with a view to agreeing a fair and reasonable apportionment of responsibility for the Delay.
- 6.11 Whatever the reasons for the Delay (whether caused by the Customer or not), the Service Provider shall make all reasonable endeavours to eliminate or mitigate the consequences of the Delay.
- 6.12 Either the Customer or the Service Provider may request that a CCN be issued in accordance with clause 26, which covers the effects of the Delay.
- 6.13 Failing agreement on the Issuing of a CCN as specified in clauses 6.8 and 6.12 herein, either party may escalate the matter in accordance with the Dispute Resolution Procedure.

7 Testing and Acceptance

- 7.1** The IT System shall be delivered through Milestones and Deliverables. As part of the implementation of each Milestone or Deliverable, the IT System shall be subject to a process of Acceptance Testing.
- 7.2** Acceptance Test criteria shall be prepared by the Customer to test that the IT System (or part thereof) conforms to requirements of the Deliverables in **Part F (Tender Documents)**. The Customer shall perform transactional and functional tests together with the results expected to be achieved by processing test data, transactional and functional test scripts and any other tests the Customer deems necessary to test the IT System. The Service Provider shall not be entitled to object to the test criteria or the expected results unless the Service Provider can demonstrate to the Customer that they are not suitable for testing the IT System as aforesaid, and if accepted, the Customer shall make reasonable amendments to the test criteria and expected results.
- 7.3** The Service Provider shall for each Deliverable submit details to the Customer for testing and the parties shall follow the applicable provisions of the testing procedures below.
- 7.4** The order for Acceptance Testing is as follows, unless the context of the TEST requires otherwise, or the parties agree a different procedure for Acceptance Testing as part of the Implementation Plan:
 - 7.4.1** one or more imports of test data into the TEST system leading to a successful import of test data into the TEST system; followed by
 - 7.4.2** TEST Acceptance Testing followed when successful by the TRAIN system. Transfer configuration from TEST to TRAIN system, one or more imports of data into the TRAIN system leading to a successful import into the TRAIN system; followed by
 - 7.4.3** TRAIN Acceptance Testing, followed, when successful, by agreement to Go-Live; followed by
 - 7.4.4** implementation of the Deliverable in the LIVE environment; followed by
 - 7.4.5** transfer of configuration from TEST to LIVE system; followed by
 - 7.4.6** LIVE data import into LIVE, followed by
 - 7.4.7** LIVE Acceptance Tests, leading, when successful, to the acceptance of a Deliverable.
- 7.5** If the Customer successfully completes the requisite LIVE Acceptance Tests; the Customer shall issue a Milestone Achievement Certificate. Notwithstanding the issuing of a Milestone Achievement Certificate, the Service Provider shall remain solely responsible for ensuring that the Service Provider's solution is suitable for delivering the IT Services, and for ensuring that the IT System is implemented in accordance with the Deliverables in **Part F (Tender Documents)**. No rights of estoppel or waiver shall arise as a result of the issue of a Milestone Achievement Certificate (or Conditional Milestone Achievement Certificate).
- 7.6** The Customer shall carry out Acceptance Tests over the number of days described in the Implementation Plan.
- 7.7** If there are any failures in the Acceptance Tests, the Customer shall inform the Service Provider while the Acceptance Tests are in progress or promptly thereafter. The Service Provider shall not later than five (5) working days following notification of the relevant failure, at its own expense correct the errors and notify the Customer that it is ready to repeat the tests. The tests shall be repeated within one (1) month, or such other mutually convenient time as may be agreed by both parties.
- 7.8** In the event the IT System fails to pass the repeat tests referred to in clause 7.7 the Customer shall be entitled to terminate this Agreement.

- 7.9 On agreement for a Deliverable to Go-Live, the Service Provider shall deliver to the Customer the Support Materials (if any) relating to that Deliverable on appropriate media and in an appropriate format to ensure that the Customer or a third party appointed by the Customer is able to maintain, enhance, modify and change the Customer Data or other Customer's information;
- 7.10 After the acceptance of a Deliverable from clause 7.4.6, the Service Provider shall provide a warranty that the Deliverable is fit for purpose and is of a satisfactory quality and fit for its intended use.
- 7.11 Six (6) months after the last Deliverable is delivered to the LIVE environment, the Customer shall carry out Final Performance Acceptance Tests and upon successful completion, deliver to the Service Provider a written Final Performance Acceptance Certificate.

8 Support Services

- 8.1 The Service Provider shall provide the Support Services in Part B following each Go-Live.

9 Charges and Payment

- 9.1 In consideration of the IT Services being delivered or performed by the Service Provider pursuant to this Agreement, the Customer shall pay the Charges or portions thereof as described in the Pricing Matrix at Part F, 2a, Charges. Where it is agreed that payment of Charges shall be aligned to Milestones or Deliverables, the payments shall be made on delivery at the intervals or on the dates described in the Implementation Plan.
- 9.2 The Charges, including hosting and cloud services & storage shall be fixed at the rate(s) given in Part F, 2a, Charges for the period of the Initial Term, and thereafter set for each Subsequent Term and any changes in price shall reflect the changes in the amount(s) paid by the Service Provider.
- 9.3 The Charges for the Support Services (except Charges for hosting and cloud services & storage) shall be fixed for the Initial Term and shall be inclusive of all costs and expenses incurred by the Service Provider in providing IT Services.
- 9.4 For Subsequent Terms, any increase in the Charges for Support Services (except Charges for hosting and cloud services & storage) may only be increased annually in line with inflation as measured by the Consumer Prices Index, up to a maximum of 1.5% of the total IT Support Service Charges.
- 9.5 The Service Provider shall invoice the Customer for the Charges in the amounts and at the rates and frequency set out in the Pricing Matrix at Part F, 2a, Charges or as agreed in the Implementation Plan. All invoices and payment communications must quote the Purchase Order number stated on the Order Form.
- 9.6 The Charges payable by the Customer shall be paid within thirty (30) days after receipt of a valid invoice by the Customer.
- 9.7 The Charges stated in this Agreement are exclusive of any applicable VAT or other sales tax which shall be payable by the Customer at the rate and in the manner prescribed by law on submission of a valid tax invoice.
- 9.8 All invoices shall be accompanied by supporting documentation and a breakdown of the costs.
- 9.9 Payment by the Customer shall be without prejudice to any claims or rights the Customer may have against the Service Provider and shall not constitute an admission by the Customer as to

the performance of the Service Provider's obligations under this Agreement.

10 Warranties

10.1 The Service Provider warrants that the performance, and functionality of the Software will conform at all times with the Tender Documents.

10.2 The Service Provider warrants and undertakes to the Customer that:

- 10.2.1** it shall provide the IT Services with all reasonable skill and care, using suitably skilled personnel;
- 10.2.2** it has sufficient experience of installing, developing and integrating IT systems;
- 10.2.3** its employees, agents and sub-contractors shall be suitably experienced to perform their tasks/roles and conform to the standards, skill and ability to be reasonably expected of such performance;
- 10.2.4** neither the execution nor the performance of this Agreement shall conflict with any agreement or arrangement to which the Service Provider is a party or any legal or administrative arrangement by which the Service Provider is bound;
- 10.2.5** it is authorised to use the Third-Party Software and any third-party systems in connection with its obligations under this Agreement and shall remain so authorised for the duration of this Agreement and shall be authorised by the relevant licensors and owners to grant the rights for the Customer's use;
- 10.2.6** none of the IT Services, Support Materials or the IT System provided by the Service Provider shall include:
 - 10.2.6.1** any executable code in the Live system which has not passed the Acceptance Tests by the Customer; or
 - 10.2.6.2** malware, such as computer viruses, worms, time bombs, or 'trojans' or any other such devices or mechanisms of misuse;
- 10.2.7** From each Go-Live Date:
 - 10.2.7.1** the IT Services shall conform in all respects with the appropriate Deliverables in **Part F, 1, Deliverables**);
 - 10.2.7.2** the Support Materials shall provide adequate instructions to enable the Customer to make proper use of the facilities and functions; and
 - 10.2.7.3** the IT Services shall operate fully with the Software and Third-Party Software and third-party systems.
- 10.2.8** the Support Services shall comply with the Service Levels in the Service Level Agreement at **Part B**;
- 10.2.9** the capacity of the IT System is capable of meeting the transaction, connection, uptime and concurrent users' volumes described in **Part F, 1, Deliverables**;
- 10.2.10** the Service Provider has and shall maintain in effect all necessary licences and any other authorisations and rights required in providing IT Services, including those to the enhancements, modifications and upgrades to Third Party Software;
- 10.2.11** the Software, the IT Services and other materials designed or developed or produced by the Service Provider shall not infringe any third party's Intellectual Property Rights, shall not be obscene or defamatory, and shall comply with all applicable laws, regulations and codes of conduct;

- 10.2.12 each Deliverable shall meet the Customer's acceptance criteria as identified in the **Part F, Tender Documents**.
- 10.3 If the Service Provider receives written notice from the Customer at any time after any Go-Live Date of any breach of the warranties herein stipulated, the Service Provider shall immediately after receiving such notice remedy the defect or error in question.
- 10.4 The Customer warrants that all Intellectual Property Rights including but not limited to Customer's software, databases, graphics, diagrams, charts, sound, and Customer Data which shall be used and/or which is necessary for the Service Provider to access and use, is either the Customer's property or is legally licensed to the Customer to permit access and use by the Service Provider.
- 11 Service Provider's Obligations**
- 11.1 The Service Provider shall provide IT Services:
- 11.1.1 with skill and expertise to a professional standard;
- 11.1.2 which are fit for their intended purpose;
- 11.1.3 in a timely and efficient manner;
- 11.1.4 using suitably experienced personnel;
- to meet the Customer's business requirements and in accordance with this Agreement.
- 11.2 In addition, the Service Provider shall:
- 11.2.1 to the extent that a standard is not specifically described, ensure the Deliverables are of a satisfactory quality and fit for its intended use, whether expressly or by implication made known to the Service Provider;
- 11.2.2 ensure continuing integration with the Customer's existing systems identified by the Customer, and seamlessly interfaces to the Customer's and third-party systems as specified in the **Deliverables (Part F, 1, of Tender Documents)**;
- 11.2.3 co-operate with the Customer's officers, employees and other independent consultants whenever necessary or desirable in the performance of IT Services;
- 11.2.4 comply with all reasonable instructions given by the Customer's Representative and notify the Customer's Representative promptly if the Service Provider has any difficulty in complying with any instruction, or if there is any conflict, ambiguity or discrepancy in the Tender Documents which has not been identified before the award of the contract to the Service Provider;
- 11.2.5 comply with all applicable UK and European laws, directives and regulations, and any amendments thereto, which apply to IT Services now or which come into force during this Agreement;
- 11.2.6 comply with the Customer's financial and contractual standing orders, financial regulations, financial control standards, and policies and procedures, as notified to the Service Provider from time to time;
- 11.2.7 ensure that IT Services are delivered respecting the Pricing Matrix at **Part F, 2a, Charges**;
- 11.2.8 provide project management for the delivery of IT Services as described in the **Deliverables (Part F, 1, of Tender Documents)**;

- 11.2.9 provide the necessary personnel to work alongside the Customer and provide timely feedback and any necessary information;
 - 11.2.10 ensure that key personnel are not removed or replaced without prior agreement of the Customer from the performance of the IT Services during the dates they are required in this Agreement;
 - 11.2.11 ensure that the Service Provider's personnel comply with the Customer's requirements for the conduct of staff when on the Customer's premises.
- 11.3 The Service Provider shall appoint a Representative and Key Personnel (Identified in Part I) who are assigned to oversee the performance and successful delivery of the IT Services. The Service Provider may change the Service Provider's Representative and Key Personnel with the prior written consent of the Customer, such consent not to be unreasonably withheld or delayed.
- 11.4 Where the Service Provider has purchased Third Party Software, the Service Provider shall pay for the Third-Party Software within the time allowed by the third party and shall not put at risk the Customer's possession and use of the Third-Party Software after delivery to the Customer.
- 11.5 The Service Provider undertakes to maintain the interface and interoperability between Third Party Software and Software developed or provided by the Service Provider.
- 11.6 The Service Provider shall take all appropriate steps to ensure that the Service Provider's personnel are not in a position where there is or may be a conflict of interests between the Service Provider's personnel and another contractor where both are providing IT Services to the Customer under this Agreement.
- 11.7 The Service Provider shall, as a continuing obligation throughout the term of this Agreement, where Software is used in the provision of IT Services or information uploaded, interfaced or exchanged with the Customer's systems, use the most up-to-date antivirus from an industry-accepted antivirus software vendor. The Service Provider shall check for, contain the spread of, and minimise the impact of malicious software.
- 11.8 If malicious software is found, the Service Provider shall co-operate with the Customer to reduce the effect of the malicious software. If malicious software causes loss of operational efficiency or loss or corruption of the Customer Data, the Service Provider shall use its best endeavours to help the Customer to mitigate any losses and restore the provision of IT Services to the desired operating efficiency as soon as possible.

12 Customer Obligations

- 12.1 The Customer acknowledges that the Customer's close involvement is essential to ensure that the IT Services successfully meet the Customer's requirements.
- 12.2 The Customer agrees to provide guidance to the Service Provider on the Customer's business practices which affect IT Services.
- 12.3 The Customer shall pay for IT Services delivered under and in accordance with this Agreement.
- 12.4 The Customer shall appoint a Representative and Key Personnel (identified in Part I) who are assigned to oversee the successful performance and delivery of the IT Services. The Customer may change the identity of the Customer's Representative or any of the details of the Customer's Representative and Key Personnel on written notice to the Service Provider.
- 12.5 If requested by the Service Provider, the Customer shall provide a desk and wi-fi facilities for the use of the Customer on a licence-at-will basis.

13 Termination

Termination for Convenience

- 13.1** Notwithstanding any other term, the Customer may terminate this Agreement by giving at least six (6) months' prior written notice to the Service Provider, notice to expire at the end of the Initial Term or, if later, a Subsequent Term.

Termination for Material Breach

- 13.2** The Customer may terminate this Agreement forthwith on giving notice in writing:

13.2.1 if the Service Provider is in breach of:

- 13.2.1.1** clause 19 (Confidential Information);
- 13.2.1.2** clause 20 (Customer Data and Data Protection);
- 13.2.1.3** clause 21 (Freedom of Information);
- 13.2.1.4** clause 22 (Security and Control);
- 13.2.1.5** clause 23 (Compliance).

13.2.2 If the Service Provider fails to:

- 13.2.2.1** deliver a Deliverable by its associated delivery date;
- 13.2.2.2** comply with a Correction Plan;
- 13.2.2.3** meet a Service Level target;
- 13.2.2.4** pass the repeat Acceptance Tests;

13.2.3 If the Service Provider's level of performance causes a Critical Fault as defined in **Part B**;

13.2.4 if the Service Provider commits a Material Breach, of any term of this Agreement and (in the case of a breach capable of being remedied) shall have failed within fourteen (14) days after the receipt of a request in writing from the Customer to do so, to remedy the breach (such request to contain a notice of the Customer's intention to terminate);

- 13.3** The Service Provider may terminate this Agreement forthwith on giving notice in writing if the Customer commits a breach of its obligation to pay undisputed Charges by giving the Customer ninety (90) days written notice specifying the breach and requiring its remedy (such request to contain a warning of the Service Provider's intention to terminate);

Termination for Insolvency

- 13.4** Either party may terminate this Agreement forthwith on giving notice in writing if the other party is involved in any legal proceedings concerning its solvency, or ceases trading, or commits an act of bankruptcy or is adjudicated bankrupt or enters into liquidation, whether compulsory or voluntary, other than for the purposes of an amalgamation or reconstruction, or makes an arrangement with its creditors or petitions for an administration order or if a receiver or manager is appointed over all or any part of its assets or if it generally becomes unable to pay its debts within the meaning of Section 123 or Section 268 of the Insolvency Act 1986;

Termination for Change of Control

- 13.5** The Customer may terminate the Agreement forthwith on giving written notice (without penalty) if there is a change of control in the Service Provider to which the Customer objects, except where the Customer has given its prior written consent to the change of control, which subsequently takes place as proposed.

Termination for a Force Majeure Event

13.6 Termination for a Force Majeure event (as described in clause 29).

Termination and Accrued Rights

13.7 Any termination of this Agreement (howsoever occasioned) shall not affect any accrued rights or liabilities of either party.

14 Consequences on Expiry or Termination

14.1 Following the service of a termination notice for any reason, the Service Provider shall continue to be under an obligation to provide IT Services to the required Service Levels and to ensure that there is no degradation in the standards of IT Services until the date of termination.

14.2 On expiry or termination of this Agreement for any reason the Service Provider shall:

14.2.1 repay to the Customer any Charges or other sums paid in advance in respect of IT Services not provided as at the date of expiry or termination.

14.2.2 co-operate with the Customer's requirements to return, destroy or delete (or to procure the return, destruction or deletion thereof) all:

14.2.2.1 the Customer's Confidential Information under its control or in its possession;

14.2.2.2 the Customer Data, or media containing the Customer Data or other materials provided by the Customer; and

14.2.2.3 the Customer owned property in the possession or control of the Service Provider or its sub-contractors, to the Customer;

and to deliver to the Customer a Certificate of Return, Destruction or Deletion signed and dated by a board director.

Migration Services

14.3 The Service Provider shall work with the Customer and ensure an orderly transition of the IT Services to the replacement Service Provider.

14.4 On expiry or termination of this Agreement for any reason, the Customer may request the Service Provider to provide migration services to the Customer or to a third-party service provider identified by the Customer at no charge to the Customer for thirty (30) days (and thereafter at a reasonable fee to be agreed with the Customer).

14.5 Where the Customer requests migration services, the Service Provider shall deliver the Customer Data in an agreed format to the Customer or to any successor ISP address(es) and location(s) designated by the Customer;

14.6 The Customer shall accept the migration services within 60 days after delivery of the Customer Data and the Software to the Customer or its nominee as provided for in this Agreement or on notice of acceptance to the Service Provider whichever is the earlier. On such acceptance, the Service Provider shall not be obliged to provide any further migration services to the Customer.

14.7 The Customer shall, on termination or at the end of the migration services (if later), return to the Service Provider any Software or media that is owned by the Service Provider or third-party licensor if applicable, provided that the Customer may retain a copy for audit purposes.

15 Liability, Indemnity and Limitations

15.1 Notwithstanding any other provision in this Agreement, the Service Provider neither excludes nor limits liability to the Customer for any claims, losses (including regulatory losses and fines),

damages, costs or expenses, or acts or omissions arising from:

- 15.1.1 the negligence of the Service Provider, its officers, employees, agents and sub-contractors in the performance of their duties, resulting in death or personal injury;
 - 15.1.2 bribery, fraud or fraudulent misrepresentation;
 - 15.1.3 the Service Provider's Intellectual Property Rights indemnities;
 - 15.1.4 breaches of Data Protection Legislation; and
 - 15.1.5 any other liability which by law cannot be excluded or limited.
- 15.2 Except as provided in clause 15.1 above, the Service Provider's total liability to the Customer for any claims, losses, damages, costs and expenses arising under this Agreement or otherwise for any cause whatsoever shall be limited to the sum of the relevant insurance cover in clause 16 below.
- 15.3 The Service Provider shall, in addition, compensate the Customer for any additional operational or administrative costs and expenses resulting from a Material Breach of the Service Provider.
- 15.4 Except as otherwise prohibited by law, the Customer's total liability to the Service Provider for any claims, losses, damages, costs and expenses arising under this Agreement or otherwise for any cause whatsoever, shall be limited to the value of the monies paid to the Service Provider under this Agreement.
- 15.5 In no event shall either party be liable to the other for any loss of profits, business, revenue, damage to goodwill, savings or any indirect, special or consequential loss or damage.
- 15.6 The parties acknowledge and agree that the limitations contained in this clause 15 are commercially reasonable in the light of the nature of the IT Services, the identity of the Customer and all the relevant circumstances relating to delivery of the IT Services.

16 Insurance

- 16.1 The Service Provider shall from the Commencement Date up to the end of the Limitation Period maintain, as a minimum, the insurance policies described in the Order Form with an insurance company of repute to cover its liabilities for each and every claim.
- 16.2 The Service Provider shall notify the Customer immediately if any such insurance policy at any time ceases to be in force and shall immediately take out replacement insurance.
- 16.3 The Service Provider shall on request of the Customer immediately supply copies of the relevant certificates of insurance at any time during the continuation of this Agreement.
- 16.4 The Service Provider shall ensure that all sub-contractors hold insurances (described in clause 16.1 above) of the same amounts that the Service Provider would be legally liable to pay as damages, including claimant's costs and expenses.
- 16.5 Holding insurance cover shall not relieve the Service Provider of any liabilities under this Agreement.
- 16.6 The Service Provider shall take all risk control measures relating to the IT Services as would be reasonable to expect from a contractor acting in accordance with Good Industry Practice;
- 16.7 The Service Provider shall promptly notify the insurers in writing of any relevant material fact under any insurances of which the Service Provider is, or becomes, aware;

17 Intellectual Property Rights and Licences

OPTION 1

Service Provider IPR and Licences for COTS and SaaS

- 17.1 The Intellectual Property Rights of the Service Provider's Software and any modifications created outside of this Agreement is the Background IPR of the Service Provider and/or its licensors.
- 17.2 All work created by the Service Provider for and under this Agreement is the Service Provider's Foreground IPR.
- 17.3 The Service Provider grants to the Customer a licence suitable for a commercial off-the-shelf software, as amended, modified and delivered to the Customer, in accordance with and for the duration and purposes of this Agreement.
- 17.4 The Service Provider shall obtain from its third-party providers all licences for the Customer to use throughout and for the purposes of this Agreement, any Third-Party Software or systems (including hosting and cloud services & storage services) that is recommended or provided by the Service Provider.

OPTION 2

Service Provider IPR and Licences for Bespoke Work

- 17.5 The Intellectual Property Rights of the Service Provider's Software and any modifications created outside of this Agreement is the Background IPR of the Service Provider and/or its licensors.
- 17.6 All Bespoke Work created by the Service Provider for and under this Agreement vests in the Customer and is the Customer's Foreground IPR. The Service Provider grants to the Customer a perpetual, non-revocable licence in any of the Service Provider's Background IPR embedded in the Bespoke Work.
- 17.7 The Customer grants to the Service Provider a limited licence to use the Customer's Foreground IPR for the purposes of this Agreement.
- 17.8 Where the Order Form is silent on which Option applies, Option 2 shall apply in default.

Customer's IPR and Licences

- 17.9 The Intellectual Property Rights of the Customer in the Customer's software and Customer Data created outside this Agreement is the Background IPR of the Customer and/or its licensors.
- 17.10 All Intellectual Property Rights in the Customer's software and Customer Data created for and under this Agreement is the Customer's Foreground IPR.
- 17.11 The Service Provider shall have no rights to use the Customer's names, logos or trademarks without the Customer's prior written approval.
- 17.12 The Customer grants to the Service Provider a limited, non-transferable, non-exclusive, royalty-free licence to use only such of the Customer's Intellectual Property Rights as is required, solely to enable the Service Provider to deliver the IT System and to perform the Services.

Moral Rights

- 17.13 The Service Provider shall procure that all moral rights of its authors (including that of its sub-contractor's authors) arising from the performance of this Agreement are waived. The Service Provider shall indemnify the Customer in the event of any claims, actions or proceedings for any costs, losses, damages, or expenses brought by the author against the Customer.

18 Intellectual Property Infringement and Claim

- 18.1** The Service Provider shall defend at its own expense any claim brought against the Customer alleging that the use of the IT System infringes the Intellectual Property Rights of a third party ('Intellectual Property Claim') and the Service Provider shall pay all costs and damages awarded or agreed to in settlement of an Intellectual Property Claim provided that the Customer:
- 18.1.1** furnishes the Service Provider with prompt written notice of the Intellectual Property Claim;
 - 18.1.2** provides the Service Provider with reasonable assistance in respect of the Intellectual Property Claim; and
 - 18.1.3** gives to the Service Provider the sole authority to defend or settle the Intellectual Property Claim.
- 18.2** If, in the Service Provider's reasonable opinion, the use of the IT System is or may become the subject of an Intellectual Property Claim then the Service Provider shall either:
- 18.2.1** obtain for the Customer the right to continue using the IT System which is the subject of the Intellectual Property Claim; or
 - 18.2.2** replace or, with the written consent of the Customer, modify the IT System, which is the subject of the Intellectual Property Claim, so it becomes non-infringing.
- 18.3** If the remedies set out in clause 18.2 above are not in the Service Provider's opinion reasonably available, the Customer shall cease using the IT System which is the subject of the Intellectual Property Claim, the Service Provider shall repay to the Customer all sums paid to the Service Provider and indemnify the Customer for all damages, losses, costs and expenses including reasonable legal expenses and third party claims suffered by the Customer.
- 18.4** Any replacement or modification made to the IT System under clause 18.2.2 shall be subject to the same warranties and terms of this Agreement and the Customer shall have the same rights as if they were made on the Commencement Date.
- 18.5** Each party recognises that the other party's business relies upon the protection of its IPR and that in the event of a breach or threatened breach of IPR, the other party shall be caused irreparable damage and such other party may therefore be entitled to injunctive or other equitable relief to prevent a breach or threatened breach of its IPR.
- 18.6** If a party learns of any claim of infringement of the Customer's Intellectual Property Rights in the Customer Data, it shall promptly notify the other party. The Service Provider shall do all such things as the Customer may reasonably require at the Customer's expense to assist the Customer in taking proceedings or any other actions the Customer may reasonably take to terminate or prevent any such claim.

19 Confidential Information

- 19.1** Both parties to this Agreement undertake, except as provided below, to treat as confidential and keep secret all information marked 'confidential' or which may reasonably be supposed to be confidential, including, without limitation, information contained or embodied in the Deliverables in **Part F, 1 of the Tender Documents** and other information supplied by the Customer or Service Provider (in this Agreement collectively referred to as '**Confidential Information**') with the same degree of care as it employs with regard to its own confidential information of a like nature and in any event in accordance with best current commercial security practices, provided that, this clause shall not extend to any information which was rightfully in the possession of either party prior to the commencement of the negotiations

leading to this Agreement or which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause).

19.2 A party shall not without the prior written consent of the other party divulge any part of the Confidential Information to any person except:

19.2.1 to their own directors, officers, employees, sub-contractors and agents and then only to those persons who need to know the same;

19.2.2 to either party's auditors, an officer of Inland Revenue, an officer of HM Revenue and Customs, a court of competent jurisdiction, governmental body or applicable regulatory authority and any other persons or bodies having a right duty or obligation to know the business of the other party and then only in pursuance of such right duty or obligation; or

19.2.3 where it must be disclosed pursuant to a statutory, legal or parliamentary obligation placed upon the party making the disclosure, including any requirements for disclosure by the Customer under the Freedom of Information Act 2000, save where an exemption applies, or the Code of Practice on Access to Government Information or the Environmental Information Regulations apply.

19.2.4 to any person who is for the time being appointed by either party to maintain the equipment on which the Software is for the time being used (in accordance with the terms of the Agreement) and then only to the extent necessary to enable such person to properly maintain the equipment.

19.3 Both parties undertake to ensure that persons and bodies referred to in clause 19.2 are made aware before the disclosure of any part of the Confidential Information that the same is confidential and that they owe a duty of confidence to the other party.

19.4 Each party to this Agreement shall promptly notify the other party if it becomes aware of any breach of confidence by any person to whom it divulges all or any part of the Confidential Information and shall give the other party all reasonable assistance in connection with any proceedings which the other party may institute against such person for breach of confidence.

20 Customer Data and Data Protection

20.1 The Customer shall own (or shall have the right to use) all right, title and interest in and to all of the Customer Data.

20.2 The Service Provider shall comply with its Privacy and Security Policy (described in the Order Form) relating to the privacy and security of the Customer Data.

20.3 In respect of Personal Data, both parties undertake to comply with the provisions of the Data Protection Legislation, more fully described in **Part D**.

21 Freedom of Information

21.1 The Service Provider acknowledges that the Customer is subject to the requirements of the Code of Practice on Access to Government Information, the Freedom of Information Act 2000 ("FOIA") and the Environmental Information Regulations 2004 ("EIR").

21.2 The Service Provider shall assist and co-operate with the Customer in a timely and efficient manner and provide a copy of all information in its possession or power, in the form that the Customer requires, to enable the Customer to respond to a request for information within the time for compliance set out in Section 10 of the FOIA.

- 21.3 The Service Provider may request in **Part F, 2c of the Tender Documents** that certain information arising out of the execution of the works be classified as reserved information under the Freedom of Information Act 2000 ("FoIA") and the Environmental Information Regulations and not disclosable by the Customer to third parties.
- 21.4 **Part F, 2c** shall list the class or category of information or the information itself and shall specify which exemptions under the FoIA apply to each specified class category or specific information. Each case shall indicate when it is likely that the information can be made available under the FoIA or if the information is unlikely ever to be made so available that this is the case. Where such information is exempt under the rules governing commercial matters (s.43(2) FoIA) then unless special circumstances apply it shall not be withheld under the FoIA for more than seven (7) years after the expiry or termination of this Agreement.
- 21.5 Information relating to the overall value performance or completion of this Agreement, or relating to contract records and administration, shall not be accepted as reserved information. The Customer may however withhold access to such information under the FoIA in appropriate cases.
- 21.6 The Service Provider acknowledges that the Customer may, acting in accordance with the Department of Constitutional Affairs' Code of Practice on the Discharge of Functions of Public Authorities under Part I of the Freedom of Information 2000, be obliged under the Code of Practice on Access to Government Information, the FOIA, or the Environmental Information Regulations to disclose information without consulting with the Service Provider, or following consultation with the Supplier and having taken its views into account.
- 21.7 Should it subsequently transpire that any information has been incorrectly classified as reserved information by the Service Provider or any competent public authority orders the information to be released, the Service Provider shall immediately deliver such information to the Customer and reimburse all the costs incurred by the Customer as a result of the Service Provider seeking to classify the information as reserved information.
- 21.8 The Service Provider shall ensure that all information produced in the course of the Agreement or relating to this Agreement is retained for disclosure and shall permit the Customer to inspect such records as requested from time to time. The Service Provider acknowledges that any lists or schedules provided by it outlining Confidential Information are of indicative value only and that the Customer may nevertheless be obliged to disclose Confidential Information in accordance with clause 19.2.3.

22 Security and Control

- 22.1 The Customer may, during the continuance of this Agreement refuse admission to the Customer's premises of any of the Service Provider's personnel whom the Customer believes represents a security risk or require the Service Provider to exclude such personnel from working on the IT Services or IT Services under this Agreement or does not have the required levels of training and expertise or where the Service Provider has other grounds for doing so. The decision of the Customer shall be final, and it shall not be obliged to provide any reasons.
- 22.2 The Service Provider shall:
- 22.2.1 use its best endeavours to keep confidential the passwords or other security information relating to the IT Services or any equipment of the Customer;
 - 22.2.2 ensure compliance with the Customer's security requirements to protect the authenticity and integrity of the IT Services, and pro-actively provide security for the IT Services, ensuring that adequate security protections are in place;

- 22.2.3 regularly review its security policies and the actual security of the IT Services, and inform the Customer of any additional measures necessary to maximise security of the IT Services and integrity of the Customer Data, and other Customer's information;
- 22.2.4 notify the Customer promptly of any unauthorised access or use of the Customer Data or other security incident affecting its network and information systems that could potentially affect the Customer, and respond without delay to all queries and requests for information from the Customer, whether discovered by the Service Provider or the Customer, in particular bearing in mind the extent of the Customer's reporting obligations under applicable network and information security legislation and that the Customer may be required to comply with statutory or other regulatory timescales;
- 22.2.5 comply with the staffing and remote working requirements of the Customer, as required;
- 22.2.6 have in place a comprehensive Business Continuity and Disaster Recovery Policy and Procedures approved by the Customer (described in the Order Form) which are reviewed at least annually and meet the contractual RTO and RPO.
- 22.2.7 ensure that any sub-contractor or third-party provider of any of IT Services shall have similar Business Continuity and Disaster Recovery policy and procedures in place.
- 22.2.8 use all reasonable endeavours to ensure continuity of personnel and to ensure that the turnover rate of its staff engaged in the provision or management of IT Services is at least as good as at the prevailing industry norm for similar services.
- 22.2.9 promptly replace any key personnel that the Customer considers unsatisfactory at no extra charge.
- 22.2.10 promptly replace any Key Personnel (Part I) who leaves the project team working on the IT Services under this Agreement with someone who is of equivalent skills and experience in consultation with the Customer.
- 22.2.11 at the Service Provider's cost, carry out penetration tests at least once annually or sooner if required and anytime there is a significant infrastructure or application upgrade or modification.
- 22.2.12 co-operate with the Customer in all aspects of its compliance with the Network and Information Systems Regulations including, without limitation, any requests for information in the event of a suspected or actual security incident and any inspections by regulators.
- 22.3 The Service Provider and its staff shall also adhere to the Customer's business continuity and disaster recovery procedures as required.
- 22.4 The Service Provider shall comply with the Customer's Health & Safety policies and procedures while on the Customer's premises.
- 22.5 The Service Provider shall follow Good Industry Practice for storage procedures for Customer Data and shall have in place a back-up policy approved by the Customer described in the Order Form). The Service Provider shall notify the Customer of any changes that substantially or significantly differ from that which has been disclosed to the Customer at the date of this Agreement. In the event of any damage to the Customer Data, the Service Provider shall use all best endeavours to restore the lost or damaged Customer Data from the latest back-up maintained by the Service Provider.

23 Compliance

- 23.1** The Service Provider shall in the performance of the IT Services take account of any statute, statutory instrument, byelaw, relevant British Standard (or equivalent EU standard) or other mandatory requirement or code of practice and the Customer's policies, which may be in force, or come into force, during the performance of the IT Services.
- 23.2** Without limitation to clause 23.1, the Service Provider must:
- 23.2.1** comply with the provisions of the Bribery Act 2010 and, in particular, section 7 of that Act in relation to the conduct of its employees, or persons associated with it;
 - 23.2.2** not unlawfully discriminate within the meaning and scope of the Equality Act 2010;
 - 23.2.3** comply with applicable requirements of the Modern Slavery Act 2015;
 - 23.2.4** comply with the Customer's Living Wage Provisions;
 - 23.2.5** ensure that any third party to whom it sub-contracts any part of the IT Services, must comply with this clause 23.2.
- 23.3** The Service Provider warrants that it has and will maintain in place adequate procedures designed to prevent acts of bribery from being committed by its employees or persons associated with it, and must provide to the Customer at its request, within a reasonable time, proof of the existence and implementation of those procedures.
- 23.4** The Service Provider shall take all necessary steps to secure the observance of the provisions of clause 23.2 by all its employees, agents, sub-contractors and suppliers engaged in the execution of the IT Services.
- 23.5** The Customer is entitled by notice to the Service Provider to terminate this Agreement or any other contract with the Service Provider if the Service Provider or any person employed by it or acting on its behalf fails to comply with the requirements set out in clause 23.2.

24 Survivorship

- 24.1** The provisions of any clause which by implication intended to come into or continue in force on or after termination shall by its nature be deemed to survive the termination of this Agreement.

25 Agency, Partnership

- 25.1** This Agreement shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the parties other than the contractual relationship expressly provided for in this Agreement.

26 Amendments

- 26.1** This Agreement may not be released, discharged, supplemented, interpreted, amended, varied or modified in any manner except in writing signed by a duly authorised officer or Representative of each of the parties.
- 26.2** If the Customer or the Service Provider wishes to request a change to the terms of its Call-Off Contract (a "Change"), it shall give written notice of the requested Change to the other.
- 26.3** If the Customer or the Service Provider requests a Change in accordance with clause 26.2, the Service Provider shall prepare within a reasonable time two copies of a change control notice ("CCN").

26.4 Each CCN shall contain:

- 26.4.1 the title of the Change;
- 26.4.2 the originator and date of the request for the Change;
- 26.4.3 the reason for the Change;
- 26.4.4 details of the Change;
- 26.4.5 the change in capital costs, if any, of the Change;
- 26.4.6 the change in revenue costs, if any, of the Change;
- 26.4.7 a timetable for implementation of the Change;
- 26.4.8 details of the impact, if any, of the Change on other aspects of the relevant Call-Off Contract and the provision of the IT Services;
- 26.4.9 the date of expiry of validity of the CCN; and
- 26.4.10 provision for signature by the Customer and by the Service Provider.

An example of such a Change Control Notice is set out in **Part G**.

- 26.5 Following receipt by the Customer of the CCN, the Customer and the Service Provider shall discuss the CCN. Neither the Customer nor the Service Provider shall unreasonably withhold its agreement to any Change.
- 26.6 No Change shall be effective unless and until the relevant CCN is signed by or on behalf of the Customer and the Service Provider.
- 26.7 If a CCN is not signed by or on behalf of the Customer and the Service Provider on or before the date of expiry of validity of that CCN then it shall automatically expire.
- 26.8 If a CCN is signed by or on behalf of the Customer and the Service Provider on or before the date of expiry of validity of that CCN then the Service Provider shall implement the Change in accordance with the terms of the CCN and the Customer shall perform any obligations imposed on it in the CCN in accordance with the terms of the CCN or (if applicable) the relevant provisions of the Call-Off Contract, including the payment of any charges.
- 26.9 Until such time as a Change is agreed in accordance with this clause 26, the Customer and the Service Provider shall continue to perform their respective obligations under the relevant Call-Off Contract in compliance with the terms and conditions of that Call-Off Contract without taking account of the requested Change.

27 Announcements

- 27.1 The Service Provider shall not issue or make any public announcement or disclose any information regarding this Agreement unless prior written consent has been obtained from the Customer.

28 Entire Agreement

- 28.1 Except for fraud and fraudulent misrepresentation, this Agreement supersedes all prior agreements, arrangements and undertakings between the parties and constitutes the entire agreement between the parties relating to the subject matter of this Agreement. The parties confirm that they have not entered into this Agreement on the basis of any representation that is not expressly incorporated herein.

- 28.2 For the avoidance of doubt, any terms and conditions of the Service Provider which are included or referred to in any purchase order shall not apply or take precedence unless specifically accepted in writing by the Customer and referred to in this Agreement.

29 Force Majeure

- 29.1 Notwithstanding anything else contained in this Agreement, a party affected by Force Majeure shall not be liable to the other for any loss of any kind which is directly or indirectly caused by reason of any failure or delay in the performance of its obligations under this Agreement which is due to Force Majeure.
- 29.2 A party affected by Force Majeure shall:
- 29.2.1 notify the other party in writing within five (5) days of the occurrence of the event constituting Force Majeure; and
 - 29.2.2 use its reasonable endeavours to continue to perform, or resume performance of, its obligations under this Agreement for the duration of the event constituting Force Majeure.
- 29.3 If either party becomes aware of circumstances of Force Majeure which are likely to give rise to a failure or delay on its part it shall forthwith notify the other as to the circumstances and the period for which it is estimated that such failure or delay is likely to continue.
- 29.4 If a party is prevented from performance of its obligations under this Agreement for a continuous period of more than six (6) weeks by reason of Force Majeure, the other party may terminate this Agreement immediately on service of written notice upon the party so prevented.
- 29.5 Any costs arising from such delay shall be borne by the party incurring the same.

30 Notices

- 30.1 All notices under this Agreement shall be in writing.
- 30.2 Notices shall be deemed to have been duly given:
- 30.2.1 when delivered, if delivered by courier or other messenger (including registered mail) during normal business hours of the recipient; or
 - 30.2.2 when sent, if transmitted by fax or e-mail and a successful transmission report or return receipt is generated; or
 - 30.2.3 on the fifth (5th) business day following mailing, if mailed by national ordinary mail, postage prepaid; or
 - 30.2.4 each case addressed to the most recent address, e-mail address, or facsimile number notified to the other party.

31 Severance

- 31.1 If any provision of this Agreement is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from this Agreement and rendered ineffective as far as possible without modifying the remaining provisions of this Agreement and shall not in any way affect any other circumstances of or the validity or enforcement of this Agreement.

32 Assignment

- 32.1 This Agreement is personal to the Service Provider and neither this Agreement nor any rights, licences or obligations under it, may be assigned by the Service Provider, without the prior written approval of the Customer.

33 Waiver

- 33.1 No delay, neglect or forbearance on the part of either party in enforcing against the other party any term or condition of this Agreement shall either be or be deemed to be a waiver or in any way prejudice any right of that party under this Agreement. No right, power or remedy in this Agreement conferred upon or reserved for either party is exclusive of any other right, power or remedy available to that party.

34 Duplicates

- 34.1 This Agreement shall be executed in duplicate, each of which shall be an original, and the duplicates shall together constitute one and the same agreement.

35 Sub-Contracting

- 35.1 With the prior written consent of the Customer (which consent shall be at the sole discretion of the Customer) the Service Provider may perform any or all of its obligations under this Agreement through agents or sub-contractors, provided always that the Service Provider shall remain fully liable for the performance and Deliverables of the sub-contractor, agent or any third party appointed by the Service Provider.
- 35.2 The Service Provider shall make its sub-contractors, agents and third parties aware of the Customer's Living Wage Provisions, and the need for the sub-contractor, agent or third party to complete (if requested by the Customer) any documentation to ensure compliance of the City's Living Wage Provisions by any third party in respect of any part of the IT Services which shall be sub-contracted by the Service Provider to any third party.
- 35.3 Sub-contracting the IT Services shall not entitle the Service Provider to charge an administration fee nor require the Customer to enter into an agreement with the third-party. All requisite third-party licences shall be held by the Service Provider for the benefit of the Customer.
- 35.4 The Service Provider shall indemnify the Customer against any loss or damage suffered by the Customer arising from any act or omission of such agents or sub-contractors.

36 Language

- 36.1 This Agreement is made only in the English language. If there is any conflict in the meaning between the English language version of this Agreement and any version or translation of it in any other language, the English language version shall prevail.

37 Costs and Expenses

- 37.1 Each party shall bear its own legal costs and other costs and expenses arising in connection with the drafting, negotiation, execution and registration (if applicable) of this Agreement.

38 Set-Off

- 38.1 Neither party may set off any liability against any sum that would otherwise be due to the other party under this Agreement.

39 Third Parties

- 39.1 A person who is not a party to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

40 Non-Poaching of Staff

- 40.1 Each party covenants with the other party that it shall not either during the term of this Agreement or within a period of twelve (12) months thereafter directly or indirectly entice away or endeavour to entice away from the other party any person who has during the previous twelve (12) months been employed by the other party involved in the performance of this Agreement.

41 Parent Company Guarantee

- 41.1 If required by the Particulars, the Service Provider shall deliver to the Customer a Deed of Guarantee (in the form set out in Part E) executed by its parent company, or where the Service Provider is part of a group of companies, then the ultimate parent holding company agreed by the Customer. The issuing of a valid parent company Deed of Guarantee shall be a condition precedent to the execution of this Agreement.

42 Limitation Period

- 42.1 The Limitation Period is six (6) years if the Agreement signed under hand, and twelve (12) years if the Agreement executed as a Deed, commencing from either the date of completion of the IT Services, or (if earlier) the date upon which the Service Provider's engagement is terminated.

43 Alternative Dispute Resolution Procedure

- 43.1 If any dispute arises in connection with this Agreement, a director or other senior representative of the parties with authority to settle the dispute shall, within 14 days of a written request from one party to the other, meet in good faith to resolve the dispute.
- 43.2 If the dispute is not wholly resolved at that meeting, the parties agree to enter into mediation in good faith to settle such a dispute and will do so in accordance with the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure. Unless otherwise agreed between the parties within fourteen (14) days of notice of the dispute, the mediator will be nominated by CEDR. To initiate the mediation a party must give an Alternative Dispute Resolution notice in writing ('ADR Notice') to the other party, referring the dispute to mediation. A copy of the referral should be sent to CEDR.
- 43.3 Unless otherwise agreed, the mediation will start not later than twenty-eight (28) days after the date of the ADR Notice.
- 43.4 No party may commence any arbitration or legal proceedings in relation to any dispute arising out of this agreement until it has attempted to settle the dispute by mediation and either the

mediation has terminated or the other party has failed to participate in the mediation, provided that the right to issue proceedings is not prejudiced by a delay.

44 Law and jurisdiction

- 44.1** This Agreement and all matters arising from it, including dispute resolutions, shall be governed by and construed in accordance with the Laws of England, and the parties submit to the exclusive jurisdiction of the English Courts.

PART B
SUPPORT AND MAINTENANCE SERVICE LEVEL AGREEMENT (SLA)

1 This SLA describes the minimum level of support and maintenance services to be provided by the Service Provider to the Customer and the respective obligations of the parties.

2 SLA Definitions

2.1 The definitions in this Part B shall supplement the definitions in Part C, as follows:

24x7 Support Hours	is as stated in the Order Form;
Core Support Hours	is as stated in the Order Form;
'Downtime'	means any service interruption of one (1) minute or more in the availability to the IT System, but shall not include any planned Outage or any service interruption where the Fault lies with the Customer;
'Extended Support Hours'	is as stated in the Order Form;
'Fault'	Any failure of the Software or IT System to operate in any material respect in accordance with the Specification and Response in Part F (Tender Documents) and Agreement, including any failure or error referred to in the Service Level Table. Fault is categorised in paragraph 3.13 below;
'Help Desk Support'	Support provided by help desk technicians sufficiently qualified and experienced to identify and resolve the support issues relating to the Software or the IT System;
'Higher-Level Support'	Support provided by persons who are more qualified or experienced to provide support at a higher level than the previous level of support given;
'Outage(s)'	includes emergency and previously scheduled windows for maintenance of the IT System;
'Permitted Purpose'	in the case of reverse analysis where permitted by applicable law, the Customer may decompile the Software if it is essential to do so in order to achieve interoperability of the IT System with another software program or media;
'Release'	means any improved, modified or corrected version or upgrade, whether major or minor, of any of the IT System, Software or media or Support Materials from time to time issued by the Service Provider;
'Service Credits'	the sum of money paid or services-in-kind provided by the Service Provider to the Customer where the Service Provider has failed to reach a Service Level target;

'Service Level Table'	The table in paragraph 9.1 below;
'SLA'	This Service Level Agreement;
'Support Period'	The period from Go-Live until expiry or termination of the Agreement and any period thereafter during which the Customer has requested the Service Provider to provide migration services;
'Support Request'	A request made by the Customer for support of the Software or IT System, including the correction of a Fault;
'Support Services'	Maintenance of the Software and IT System, including Help Desk Support and Higher-Level Support, If required
'Support Hours'	means any one or more of the Core Support Hours, the Extended Support Hours and the 24x7 Support Hours, elected by the Customer in the Order Form, for the support of the IT Services.
'Uptime'	is all time that is not Downtime.

3 Support Services:

3.1 The Service Provider shall provide the following Support Services, comprising:

- 3.1.1 software support and maintenance;**
- 3.1.2 hosting support and maintenance;**
- 3.1.3 technical support;**
- 3.1.4 service recovery;**
- 3.1.5 Help Desk Support, including the provision of Higher-Level Support;**
- 3.1.6 training;**
- 3.1.7 Support Materials; and**
- 3.1.8 such other support services as a reasonable service provider would be expected to provide from time to time.**

3.2 During the Support Period, the Service Provider shall perform the Support Services to ensure that the IT System is maintained and operating efficiently and effectively to meet the Customer's requirements during the Support Hours in accordance with the Service Levels.

3.3 In the event the IT System becomes unavailable, the Service Provider shall remedy the Fault, in accordance with this SLA.

3.4 The Service Provider shall give the Customer notice in accordance with the specification of any planned maintenance work which shall affect the availability of the IT System and shall plan and carry out such work at such times so as to minimise disruption to the availability of the IT System.

3.5 This SLA shall be read in conjunction with the other terms and conditions of the Agreement relating to the delivery of the IT Services.

- 3.6 As part of the Support Services, the Service Provider shall:**
- 3.6.1 Monitor the system for availability and Faults**
 - 3.6.2 Use all reasonable efforts to correct Faults notified to or identified by the Service Provider;**
- 3.7 The Support Services shall include:**
- 3.7.1 information and advice by telephone, email or via the Service Provider's support website;**
 - 3.7.2 information and advice by telephone, email or via the Service Provider's support website on Releases;**
 - 3.7.3 upon request by the Customer, the diagnosis of Faults in the IT System, Software or media and the rectification (in accordance with paragraph 12.5 below) of such Faults remotely (or if the Customer considers necessary, by attendance on the Customer's site) by the issue of fixes in respect of the IT System, Software or media and the making of all necessary consequential amendments (if any) to the Support Materials;**
 - 3.7.4 the creation and despatch to the Customer from time to time of patches and fixes;**
- 3.8 The Customer may request Support Services by way of a Support Request. The Support Request shall contain a detailed description of the problem or Fault and where known the start time of the incident. The Customer shall telephone or document to the Service Provider a detailed description of any Fault requiring Support Services and the circumstances in which it arose, forthwith upon becoming aware of the same, so that it can be replicated. The Customer shall provide such additional information as may be reasonably requested by the Service Provider to enable the Fault to be classified in accordance with paragraph 3.13 below.**
- 3.9 The Service Provider shall:**
- 3.9.1 Prioritise all Support Requests based on its reasonable assessment of the severity level of the problem reported; and**
 - 3.9.2 Respond to all Support Requests in accordance with the responses and response times specified in the table set out below.**
- 3.10 Where Help Desk Support is not provided within the relevant Service Level response**
- 3.11 time, the Service Provider shall escalate the Support Request to Higher Level Support;**
- 3.12 Support Services shall be provided during the Support Hours. Out of hours emergency support for Critical Faults will be provided on a best endeavours basis and to meet the resolution times of the table in paragraph 3.13 below.**
- 3.13 Support Services shall be provided in accordance with the following procedure and timescales:**

'Critical Fault'	means any fault which is fatal, or disables major functions of the Customer's business or marketability of its services or products which results in the IT System, Software or media being non-operational for business-critical delivery;
'Major Fault'	means a Fault which has a severe impact in any part of the IT System, Software or media which does not constitute a Critical Fault, but which prevents the Customer operating a material part of its business for which it purchased the IT System;

'Important Fault'	means a Fault which has degraded operations or errors disabling only certain non-essential functions and which is agreed to be important by the Service Provider and the Customer but does not constitute a Critical Fault or a Major Fault;
'Minor Fault'	means a Fault which has minimal impact and is agreed to be minor by the Service Provider and the Customer, but which does not constitute a Critical Fault, Major Fault or Important Fault (for example errors in documentation and spelling errors in non-public facing forms/screens);

The following response targets are the Customer's guideline requirements:

(a) Faults reported to the Service Provider during Core Support Hours
(all times relate to times in Core Hours)

Classification of Fault	Maximum Response Time*	Progress Update Frequency	Maximum Resolution Times**
Critical Fault	30 minutes	Every 1 (ONE) hour	1 hour
Major Fault	1 hour	Every 2 hours	4 hours
Important Fault	4 hours	Every 2 days	End of next business day
Minor Fault	8 hours	Every 7 days or as otherwise mutually agreed between the parties	1 week***

(b) Faults reported to the Service Provider during Extended Support Hours
(all times related to times in Extended Support Hours)

Classification of Fault	Maximum Response Time*	Progress Update Frequency	Maximum Resolution Times**
Critical Fault	4 hours	Every 1 (ONE) hour	8 hours
Major Fault	6 hours	Every 4 hours	8 hours
Important Fault	6 hours	Every 2 days	End of next business day

Minor Fault	8 hours	Every 5 days or as otherwise mutually agreed between the parties	1 week***
-------------	---------	--	-----------

** The first response from the Service Provider by telephone or email generated by a human being (as opposed to an automated "we have received your report and will deal with it" response).*

*** A Fault is resolved when the full functionality of the system is restored. A Fault may be resolved though application of a workaround.*

Workarounds

The Service Provider will within the Maximum Resolution Time agree with the Customer an acceptable workaround that can be used until such a time that the Service Provider is able to implement a permanent fix and agree with the Customer a timescale for the implementation of a permanent fix. While the permanent fix is pending the Service Provider shall include in all performance review documents progress towards implementation and either confirm the expected implementation date or propose for the agreement of the Customer a revised implementation date.

- 3.14 If the parties agree a Fault classification, the Service Provider shall use all reasonable endeavours within the Resolution Times of such agreement (or sooner if reasonably practicable) to fix the Fault and/or supply instructions to the Customer, which are intended to provide a work around acceptable to the Customer for the Fault or provide a correction.
- 3.15 If the parties, acting with due diligence, are unable to agree on the designation of a Fault reported by the Customer pursuant to paragraph 3.4 above, the Service Provider shall, acting reasonably, designate the level of Fault and references to "agree" and "agreement" in paragraph 3.14 above shall be deemed to refer to the designation of the Fault by the Service Provider; and
- 3.16 In the event that the Customer disagrees with the designation of the Service Provider pursuant to paragraph 3.15, it shall be entitled to escalate the designation in accordance with the provisions of paragraph 6 below.
- 3.17 In order for the Service Provider to be able to provide the Support Services to the Customer, the Customer shall:
 - 3.17.1 ensure that appropriate arrangements are put into place to allow remote access to the IT System, acceptable to the parties, or where remote access is not possible, to provide physical access to such premises of the Customer as the Service Provider shall reasonably require, unless the instruction or requirement can be performed by the Customer at the direction of the Service Provider;
 - 3.17.2 to continue to maintain any IT System requirement in accordance with the minimum operating requirements from time to time as notified by the Service Provider or the owner thereof.
- 3.18 The Customer shall ensure that staff are properly and adequately trained to a level of competence in relation to the IT System, in accordance with Service Provider's guidelines on training.
- 3.19 The Service Provider shall give the Customer regular updates of the nature and status of its efforts to correct any Fault and monthly reports as to achievement of Service Levels and Service Credits to which the Customer has become entitled.
- 3.20 The Service Provider shall in respect of Critical and Major Faults report to the Customer and the Service Provider shall provide an update of work being undertaken to circumvent or provide a

correction to the Fault at least once a day, the first such update to be provided within one (1) Hour of the designation of the Fault as a Critical Fault, or such other frequency as shall be agreed between the parties from time to time.

4 Downtime and Outages

- 4.1 The Service Provider shall investigate all Downtime events by using suitably qualified personnel after becoming aware of it and shall remedy the Downtime event as soon as reasonably practicable.
- 4.2 The Service Provider shall within 2 working days provide to the Customer a report of the outcome of all Downtime investigations together with details of the actions taken, or to be taken, to prevent a repeat event. Where the report contains actions to be taken the Service Provider shall within 2 working days provide to the Customer a revised report when those actions have been undertaken. So long as actions remain to be taken the Service Provider shall provide a revised report to the Customer at intervals of not more than a week.
- 4.3 The Service Provider shall make all commercially reasonable efforts to provide the Customer with prior email notification of all scheduled and emergency Outages in accordance with the Specification.

5 Business Continuity & Disaster Recovery

5.1 Invocation

Either the Service Provider or the Customer may invoke the Business Continuity / Disaster Recovery Plan when there is either (a) a Critical Failure which has lasted, or is reasonably expected to last, longer than 1 day and the other party agrees to the invocation; or (b) a Critical Failure has lasted, or is expected to last, more than 3 days.

Where appropriate there may be a partial invocation of the Business Continuity / Disaster Recovery Plan in the event of a Major Fault (e.g., for the Public Access element of the system).

5.2 Standards

The Service Provider shall achieve the Recovery Time Objective of 24 (elapsed) hours and the Recovery Point Objective of 15 (elapsed) minutes.

6 Escalation and Reporting

- 6.1 The Customer shall be entitled to escalate any disagreement as to a designated Fault level by the Service Provider (as referred to in paragraph 3.13 above) to the Service Provider's Help Desk Supervisor and thereafter if the Customer remains dissatisfied with the designated Fault level, it shall be entitled to escalate the dispute to the following employees of the Service Provider:

- 6.1.1 to the Support Manager; and

- 6.1.2 to the Customer Services Director, or equivalent, thereafter;

the above process shall not preclude the Customer from contacting the account manager at any point during the escalation process to discuss the disagreement and, for the purposes of this paragraph 6.1, the Service Provider shall on request from the Customer notify the Customer of the identity of the individuals holding each of those positions. If resolution is not reached, the parties can escalate the matter under the Dispute Resolution Procedure.

- 6.2 Notwithstanding the Customer exercising its right to escalate the dispute in accordance with paragraph 6.1 above, the Service Provider shall continue to work towards the provision of a work around or correction of such Fault.

7 Service Credits

- 7.1 Where, at the end of each month, the Service Provider fails to provide a Solution within the relevant response/resolution times, the Customer shall become entitled to the Service Credits specified in the Performance Measuring Table (in paragraph 9.1 below) corresponding to the relevant severity level of Fault, and the Service Provider shall pay the relevant Service Credits to the Customer.

8 Performance Monitoring

- 8.1 The Service Provider shall put in place and accurately document all processes for the identification of performance against the Service Levels against the Key Performance Indicators.
- 8.2 The Service Provider's performance in meeting the Service Levels shall be reported, monitored and assessed quarterly.
- 8.3 In addition to providing Service Level reports, the Service Provider shall measure and provide such data as is reasonably required by Customer for the purposes of monitoring the Service Provider's performance in meeting the Service Levels and any other contract obligations.
- 8.4 The Service Provider shall be responsible for ensuring that all Service Level reports are accurately prepared, using up to date and accurate data. Any absence of performance data from said reports may at Customer's discretion be deemed a maximum accrual of Service Credits to which the inaccurate and/or unavailable performance data relates.
- 8.5 Where the Service Provider believes there are mitigating circumstances for the inaccurate and/or unavailable performance data, the Service Provider may present to Customer within 5 Working Days of the date the performance data or report was due:
- A. Reasons why this performance data is inaccurate and/or unavailable;
 - B. What actions will be taken to ensure it will be accurate and/or available in the future; and
 - C. Provide reasonable evidence that the relevant Service elements were not adversely affected during the period of unavailable/inaccurate performance data, then:

The Customer may, at its absolute discretion and without prejudice consider all reasonable requests and agree a reduced level of required performance in relation to such performance data for the duration that it was missing, or the Customer may reject such requests.

9 Performance reporting

- 9.1 The Service Provider shall, at no charge to the Customer, submit the following reports:

Type of report	Frequency	Information to be included in the report
Service and Service Levels performance	Monthly (and within 5 Working Days of the month end)	Service performance per KPI for each month of the previous month.

		<p>Full details of any Critical Fault and Major Fault incidents occurring wholly or partially within the previous month.</p> <p>Number of Root Cause Analysis issued with details</p> <p>Service Credits calculations</p> <p>Highlight any recurrent issues which have become problems and describe problem management actions</p> <p>Any recommendations to assist performance improvement</p>
--	--	---

10 Measurement Procedures and Tools

10.1 The Service Provider shall within 1 (ONE) month of the Commencement Date provide to the Customer full details of its measurement and monitoring tools and procedures used to:

10.1.1 measure and report Service Provider's performance of the Services against applicable Service Levels; and

10.1.2 verify performance of the Services and the carrying out its obligations of this Agreement.

11 Key Performance Indicators

11.1 Availability during Support Hours

"Downtime" means the total time during the Support Hours in the calendar month during which the service is not available excluding (i) permitted downtime during the same hours and (ii) time during the same hours during which the service is not available due to a Fault which lies with the Customer. ("X")

"Measured Period" means the total time during the Support Hours in the calendar month. ("Y")

"Supported Hours Uptime percentage" means uptime expressed as a percentage, calculated in accordance with the following formula:

$$\text{Supported Hours Uptime Percentage} = (Y - X) / Y \times 100$$

11.2 Availability outside Support Hours

"Downtime" means the total time outside the Support Hours in the calendar month during which the service is not available excluding (i) permitted downtime during the same hours and (ii) time during the same hours during which the service is not available due to a Fault which lies with the Customer. ("X")

"Measured Period" means the total time outside the Support Hours in the calendar month. ("Y")

"Non-Supported Hours Uptime percentage" means uptime expressed as a percentage, calculated in accordance with the following formula:

$$\text{Non-Supported Hours Uptime Percentage} = (Y - X) / Y \times 100$$

KPI1	Service Availability during Support Hours does not fall below the contractual availability	99.9%
KPI2	Service Availability other than in Support Hours does not fall below the contractual availability	99.5%
KPI3	Resolution of Critical Faults within the contractual time	100%
KPI4	Resolution of Major Faults within the contractual time	99%
KPI5	Resolution of Important Faults within the contractual time	95%
KPI6	Resolution of Minor Faults within the contractual time	90%

12 Service Credits:

- 12.1 The Service Provider acknowledges and agrees that payment of a Service Credit by the Service Provider is a price adjustment and not an estimate of the loss or damage that may be suffered by the Customer as a result of the Service Provider's failure to meet any Service Level.
- 12.2 The Customer's right to Service Credits is in addition to, and not in substitution for, any other rights arising from the Service Provider's failure to meet the Service Levels.
- 12.3 If the actual loss incurred by the Customer, as a result of the Service Provider's failure to supply the IT Services in accordance with the Service Levels, exceeds the relevant Service Credit, the Customer shall have a right to claim damages for losses, costs and expenses suffered (subject to the provisions of clause 15 of Part A).

12.4 Service Credit Values: Availability SLA

- 12.4.1 If Availability during Support Hours is below the agreed Availability, the Customer is entitled to a price reduction, applied as a percentage of the monthly fee for the Service.
- 12.4.2 The maximum price reduction per month that can be credited to the Customer in the event of failure to meet Availability is 100% of the monthly charge for the Service. Where several Availability failures occur in the same calendar month, they shall be accumulated into one SLA breach for the purpose of Service Credit Calculation, but each Outage shall be reported separately for the purpose of Performance Reporting.
- 12.4.3 Service Credits shall be paid to the Customer quarterly.
- 12.5 The Service Provider shall provide a rectification plan for agreement by the Customer whenever it fails to meet a Service Level for the Support Services.
- 12.6 The Service Provider shall make all reasonable endeavours to meet a Service Level target within one (1) month following any failure to meet the target.
- 12.7 Failure to comply with paragraphs 4.1, 12.5 and 12.6 shall be a breach of contract.
- 12.8 If requested, the Service Provider shall deliver to the Customer a service report and management report on queries.

- 12.9** The Customer's right to receive Service Credits shall be in addition to, and not in substitution for, any other rights arising from the Service Provider's failure to provide the Services in accordance with the terms of the Agreement.

13 Releases

- 13.1** Releases shall be applied to the TEST and TRAIN systems and the Customer informed of the changes and be given a reasonable time in the circumstances to test and where necessary retrain staff before the Release is applied to the LIVE system.
- 13.2** The process for applying a Release shall include a roll-back plan capable of returning the system to the same state as before the Release was applied. Any changes to Customer Data made during the Release process shall not be lost.
- 13.3** The Service Provider shall notify the Customer in advance of any Releases that require Downtime or service interruption, and such Releases will be applied to the LIVE system at times agreed by the Service Provider and the Customer. In the event that such advance notice coincides with significant activity periods of the Customer then the parties will agree an alternative time for applying the Release (acting reasonably).

14 Audit

- 14.1** The Service Provider shall give the Customer access to carry out an audit(s) at least once a year on the Services giving to the Service Provider reasonable notice in writing.
- 14.2** The audit(s) carried out pursuant to paragraph 14.1 shall be subject to the following restrictions:
- 14.2.1** the audit shall be carried out during standard office working hours, as agreed between the parties;
 - 14.2.2** access will be provided to relevant records necessary to determine compliance with this Agreement and no access shall be provided to information relating to other customers of the Service Provider;
 - 14.2.3** the Customer will reimburse the Service Provider's reasonable costs, for any unreasonable inconvenience caused in relation to any such audit; and
 - 14.2.4** the Customer will take all steps necessary to minimise the disruption to the Service Provider's business and services to other customers.

PART C
Definitions

'Acceptance Certificate'	the certificate or confirmation issued by the Customer to the Service Provider upon successful completion of the Acceptance Tests;
'Acceptance Tests'	the tests for acceptance of the IT Services;
'Agreement'	the Agreement for the IT Services described in the Order Form comprising the Particulars, the Standard Terms and Conditions and the Special Terms and Conditions, if any;
'Background IPR'	the Intellectual Property Rights of a party which existed prior to the date of the Agreement or which has been created outside the scope or contemplation of the Agreement;
'Bespoke Work'	Work which is created solely for the Customer;
'Business Continuity and Disaster Recovery'	Described in clause 22 of Part A, and paragraph 5 of Part B;
'Change'	Defined in Clause 26.2 of Part A;
'Charges'	the charges payable by the Customer to the Service Provider for the IT Services are described in the Order Form and the Tender Documents;
'Commencement Date'	the date of commencement of the Agreement, described in the Order Form;
'Conditional Milestone Achievement Certificate'	A Milestone Achievement Certificate that is conditional on remediation of the test issues or non-conformities of the deliverables where no testing has taken place;
'Correction Plan'	a plan of steps to be taken by the Service Provider to achieve a Milestone;
'COTS Software'	Commercial Off-the-Shelf Software;
'Customer Cause'	where a Delay to a Milestone is caused either wholly or partly by the Customer's actions or omissions;
'Customer Data'	the data, information, text, media content, features, products, services, advertisements, promotions, ontology, Links, pointers, technology, software and databases for publication (including without limitation, literary, artistic, audio and visual content), including any publication or information created by or for the Customer, for the IT Services;
'Data Protection Legislation'	is defined in Part D;
'Deed of Guarantee'	a parent company guarantee, as described in Part E;

'Delay'	a Service Provider's inability to achieve a Milestone by a Milestone Date or any other delay impacting on the Implementation Plan;
'Deliverable'	that which is required to be delivered, as described in the Specification and Implementation Plan or elsewhere in this Agreement;
'Dispute Resolution Procedure'	is described in clause 43 of Part A;
'Final Acceptance Certificate'	the final sign-off by the Customer of the final Acceptance Tests;
"Force Majeure"	any event or circumstance materially and adversely affecting the performance by a party of its obligations arising beyond its reasonable control including without limitation fires, floods, acts of war, acts of terrorism and natural disasters but excluding default of suppliers or third parties (unless caused by events which would constitute Force Majeure), events and circumstances attributable to the wilful act, neglect or failure to take reasonable precautions of the affected party, its agents or employees;
'Foreground IPR'	the Intellectual Property Rights created pursuant to and in contemplation of the Agreement as part of the project;
'Good Industry Practice'	the reasonable skill and care expected from a competent information technology and telecommunications provider carrying out its obligations;
'Go-Live'	the date specified in the Implementation Plan, or such other date agreed by the parties in writing, which is the date on which a Deliverable is uploaded into the live environment and is first made operational;
'Implementation Plan'	the implementation plan for the IT Services describing the performance of the IT Services in accordance with the timetable agreed between the parties;
'Initial Term'	The period described in the Order Form starting from the Commencement Date;
'Intellectual Property Claim'	is defined in clause 18.1 of Part A;
'Intellectual Property Rights' or 'IPR'	any copyright, database rights, design rights, domain name rights, patents, trademarks or service marks and all other intellectual property rights whether registered or not, and applications for such rights;
'IT Services'	the services described in the Tender Documents (which includes the IT System), the Support Services and any other supplemental services provided by the Service Provider;
'IT System'	the IT System to be delivered as part of the IT Services;
"Key Personnel"	refers to the staff appointed by either the Customer or Service Provider to

	administer and monitor the Services generally as identified in Part I ;
'Limitation Period'	described in Clause 42 of Part A ;
'LIVE'	the live system;
'Material Breach'	a single serious breach or persistent failure to perform as required in the Agreement;
'Milestone'	A specifically agreed event that contributes either alone, or as part of a series of events, to a Deliverable described in the Implementation Plan;
'Milestone Achievement Certificate'	a certificate of completion of a Milestone, which can be either conditional or unconditional, issued by the Customer;
'Milestone Date'	the date a relevant Milestone must be completed by in the Implementation Plan;
'Order Form'	the Order Form with a Purchase Order No., forming part of the Agreement;
'Part'	a part or Schedule to this Agreement;
'Purchase Order'	The number given to the Order Form by the Customer;
'Representative'	the representative appointed by each party respectively, authorised to take decisions on behalf of such party, and named in Part I ;
'Response'	the Service Provider's Response to the Customer's Invitation to Tender together with any associated clarifications;
'Retention'	the percentage sum retained until the successful completion of the Final Performance Acceptance Tests;
'RPO'	Recovery Point Objective;
'RTO'	Recovery Time Objective;
'SaaS'	Software as a Service;
'Service Level Agreement'	the agreement in Part B which sets out the Support Services and Service Levels for the Support Services;
'Schedule'	a Part or schedule of the Agreement;
'Service Levels'	the performance standards for the Support Services in Part B ;
'Software'	the software provided or recommended by the Service Provider to be used which may be the Service Provider's proprietary software or a Third-Party Software;
'Special Conditions'	the terms which are particular to the Agreement and described in the Order Form;

'Specification'	the Customer's statement of requirements and specification of the technical and user requirements for the IT Services and Support Services identified in the Tender Documents in Part F and associated clarifications;
'Standard Terms and Conditions'	described in the Order Form;
'Subsequent Term'	the period(s) described in the Order Form commencing on an anniversary of the Commencement Date following expiry of the Initial Term or a previous Subsequent Term;
'Support Materials'	the operating manuals (including electronic), user instructions, technical literature and documentation provided to the Customer to facilitate the support of the IT Services;
'Support Services'	the activities undertaken by the Service Provider after a Deliverable has been uploaded into the Live environment to maintain and support the IT Services;
Tender Documents	the Specification, Response and Clarifications, and other information regarding the IT Services;
'TEST'	the Test system;
'Third Party Software'	software proprietary to third parties comprised in the IT Services supplied or recommended by the Service Provider;
'TRAIN'	the Training environment or Training system as the context refers;

PART D

DATA PROTECTION

GDPR CLAUSE DEFINITIONS:

Agreement: means the Agreement for the provision of the next iteration of the Police CyberAlarm, including additional functionality in respect of ingesting/enriching/categorising firewalls, analysis and event reporting, and scanning of external IP/websites of member organisations, to provide enriched intelligence source for policing and other developments, between the Common Council of the City of London (in its capacity as Police Authority for the City of London) and Pervade Software Limited commencing on 01 December 2021;

Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer take the meaning given in the GDPR;

Customer: means the Data Service Provider;

GDPR: the General Data Protection Regulation (*Regulation (EU) 2016/679*);

Data Protection Legislation: means (i) The General Data Protection Regulation (Regulation (EU) 2016/679), the Law Enforcement Directive (EU) 2016/680), the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003), the Protection of Freedoms Act 2012, and any applicable implementing laws as amended from time to time; (ii) the DPA 2018; and (iii) all applicable law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Service Provider is bound to comply about the processing of personal data and privacy;

Data Protection Impact Assessment: an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the Service Provider under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach;

Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

DPA 2018: Data Protection Act 2018;

Parties: means the parties to the Agreement;

Protective Measures: appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it;

Sub-processor: any third Party appointed to process Personal Data on behalf of the Service Provider related to this Agreement.

Service Provider: refers to the Service Provider named on the Order Form.

Service Provider Personnel: means all directors, officers, employees, agents, consultants and contractors of the Service Provider and/or of any sub-contractor engaged in the performance of its obligations under this Agreement;

Working Days: means a day other than a public or bank holiday or weekends.

GDPR CLAUSE:

1. DATA PROTECTION

- 1.1** The Parties acknowledge that for the purposes of the Data Protection Legislation, Customer is the Controller, and the Service Provider is the Processor. The only processing that the Service Provider is authorised to do is listed in **Annex 1** by Customer and may not be determined by the Service Provider.
- 1.2** The Service Provider shall notify Customer immediately if it considers that any of Customer's instructions infringe the Data Protection Legislation.
- 1.3** The Service Provider shall provide all reasonable assistance to Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of Customer, include:
 - (a)** a systematic description of the envisaged processing operations and the purpose of the processing;
 - (b)** an assessment of the necessity and proportionality of the processing operations in relation to the Services;
 - (c)** an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d)** the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- 1.4** The Service Provider shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:
 - (a)** process that Personal Data only in accordance with **Annex 1**, unless the Service Provider is required to do otherwise by law. If it is so required, the Service Provider shall promptly notify Customer before processing the Personal Data unless prohibited by law;
 - (b)** ensure that it has in place Protective Measures, which have been reviewed and approved by Customer as appropriate to protect against a Data Loss Event having taken account of the:
 - (i)** nature of the data to be protected;
 - (ii)** harm that might result from a Data Loss Event;
 - (iii)** state of technological development; and
 - (iv)** cost of implementing any measures;
 - (c)** ensure that :
 - (i)** the Service Provider Personnel do not process Personal Data except in accordance with this Agreement (and in particular **Annex 1**);
 - (ii)** it takes all reasonable steps to ensure the reliability and integrity of any Service Provider Personnel who have access to the Personal Data and ensure that they:
 - (A)** are aware of and comply with the Service Provider's duties under this clause;
 - (B)** are subject to appropriate confidentiality undertakings with the Service Provider or any Sub-processor;
 - (C)** are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party

unless directed in writing to do so by Customer or as otherwise permitted by this Agreement; and

- (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
- (d) not transfer Personal Data outside of the EU unless the prior written consent of Customer has been obtained and the following conditions are fulfilled:
 - (i) Customer or the Service Provider has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46) as determined by Customer;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the Service Provider complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist Customer in meeting its obligations); and
 - (iv) the Service Provider complies with any reasonable instructions notified to it in advance by Customer with respect to the processing of the Personal Data;
- (e) at the written direction of Customer, delete or return Personal Data (and any copies of it) to Customer on termination of the Agreement unless the Service Provider is required by law to retain the Personal Data.

1.5 Subject to clause 1.6, the Service Provider shall notify Customer immediately if it:

- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
- (b) receives a request to rectify, block or erase any Personal Data;
- (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
- (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by law; or
- (f) becomes aware of a Data Loss Event.

1.6 The Service Provider's obligation to notify under clause 1.5 shall include the provision of further information to Customer in phases, as details become available.

1.7 Taking into account the nature of the processing, the Service Provider shall provide Customer with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by Customer) including by promptly providing:

- (a) Customer with full details and copies of the complaint, communication or request;
- (b) such assistance as is reasonably requested by Customer to enable Customer to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
- (c) Customer, at its request, with any Personal Data it holds in relation to a Data Subject;
- (d) assistance as requested by Customer following any Data Loss Event;

- (e) assistance as requested by Customer with respect to any request from the Information Commissioner's Office, or any consultation by Customer with the Information Commissioner's Office.
- 1.8 The Service Provider shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Service Provider employs fewer than 250 staff, unless:
 - (a) Customer determines that the processing is not occasional;
 - (b) Customer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
 - (c) Customer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 1.9 The Service Provider shall allow for audits of its Data Processing activity by Customer or Customer's designated auditor.
- 1.10 The Service Provider shall designate a data protection officer if required by the Data Protection Legislation.
- 1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Service Provider must:
 - (a) notify Customer in writing of the Intended Sub-processor and processing;
 - (b) obtain the written consent of Customer;
 - (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this Part D such that they apply to the Sub-processor; and
 - (d) provide Customer with such information regarding the Sub-processor as Customer may reasonably require.
- 1.12 The Service Provider shall remain fully liable for all acts or omissions of any Sub-processor.
- 1.13 The Customer may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).
- 1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Customer may on not less than 30 Working Days' notice to the Service Provider amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.
- 1.15 Notwithstanding any other provision in the Order, the Service Provider shall indemnify the Customer in respect of any, fine, loss, claim, action, damages or demand imposed on or suffered by the Controller as a result of any breach by the Service Provider of this Part D.

PART D - ANNEX

Processing, Personal Data and Data Subjects

1. The Service Provider shall comply with any further written instructions with respect to processing by Customer.
2. Any such further instructions shall be incorporated into this Annex.

Subject matter of the processing	The subject matter of the processing is the gathering and analysis of data, including personal data primarily in the form of IP addresses, to identify suspicious cyber activity against UK public and private sector organisations with a view to understanding the nature and scale of the cyber threat to the UK, contributing to the prevention of and protection from such threat, and enabling its investigation, disruption and the taking of diversion/enforcement action.
Duration of the processing	<p>The processing shall commence no sooner than the Commencement Date as specified in the Order Form and shall conclude upon the deletion/return of personal data following the expiry of the Initial Term, or any Subsequent Term or other permitted extension of the term of the Agreement or otherwise upon termination of the Agreement, in accordance with the requirements of Part A clause 14.2 of the Agreement and this Part D clause 1.4(e).</p> <p>It should be noted that not all categories of personal data will necessarily be processed from the outset of the duration of processing.</p>
Nature and purposes of the processing	<p>The purpose(s) of the processing are the law enforcement purposes, i.e., the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (see s31 Data Protection Act 2018).</p> <p>The nature of the processing activities includes the:</p> <ul style="list-style-type: none">• Collection;• Filtering;• Encryption;• Transmission;• Structuring;• Recording;• Storage;• Data matching/alignment;

	<ul style="list-style-type: none"> • Analysis; • Categorisation; • Scoring; • Retrieval; • Consultation; • Use; • Data sharing/disclosure; and, • Erasure/destruction. <p>Some of these activities may be conducted through machine learning.</p> <p>Other data is processed on the basis that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.</p>
Type of Personal Data	<p>The data processed will include personal data, including sensitive personal data and special category/criminal conviction and offence data (and therefore the Customer considers that the requirements of Part D, clause 1.8 are applicable).</p> <p>In respect of Police/law enforcement entity officers and staff:</p> <ul style="list-style-type: none"> • Name • .pnn/law enforcement entity email address • Force/law enforcement organisation • Rank/role • User credentials: username & password • Phone number • User group • Usage / Logging data <p>Member organisation staff/their representatives:</p> <ul style="list-style-type: none"> • Name • Organisation (name & company registration number) • Role / Job title • Business Address • Region • Telephone number • Email address

- Third party representative name
- Third party representative email address
- Payment data
- User credentials: username & password
- Passcode
- IP address
- Usage data
- Other personal data provided by member organisation staff/their representatives

Website visitors:

- IP address
- Usage data
- Site from which user visited PCA website

Individuals suspected of involvement in suspicious activity:

- IP address
- Domain visited
- Sender email address
- Sender handle
- Recipient email address
- Email subject
- Email attachment filename
- Mail ID
- Location data:
 - Continent
 - Country
 - City
 - Postcode
 - Latitude
 - Longitude,
 - Force area
 - Force region
- ISP
- IP address host

	<ul style="list-style-type: none"> • IP address owner • User agent • Connection type, including whether a VPN or TOR is being used • Device name • Device ID • Time zone • Event ID • Page sought to be accessed • Page from which user was referred to page sought to be accessed • Request type, i.e. to get/view, post etc • Conduct data • Personal data relating to criminal convictions and offences or related security measures (within the meaning of s.11(2) Data Protection Act 2018) • Scoring: geolocation confidence; conduct harm score; conduct resolvability score • Postcode <p>Other users of member organisation's network, website, web apps, etc, including staff and third parties:</p> <ul style="list-style-type: none"> • IP address • Domain visited • Sender email address • Recipient email address • Email subject • Email attachment filename • Device name • Device ID • Time zone • Country • Conduct data
--	--

Categories of Data Subject	<p>Categories of data subject are:</p> <ul style="list-style-type: none"> • Police/law enforcement entity officers and staff; • Member organisation staff/their representatives. • Individuals suspected of involvement in suspicious activity; • Other users of member organisation's network, website, web apps, etc, including staff and third parties; • Website users.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	<p>At the conclusion of the Initial Term or any Subsequent Term or other permitted extension of the Agreement, or upon termination of the Agreement, or at such time specified by the Customer prior to the conclusion of the Agreement to enable the efficient transfer of services to another provider, or (in respect of personal data of which a Service Recipient is the relevant data controller) upon the termination by the relevant Service Recipient of its Contract with the Supplier, the Supplier shall promptly return all data to the Customer and/or relevant Service Recipient or transfer them directly to the new provider and shall securely destroy all copies of data processed pursuant to the Agreement in accordance with the Customer's written instructions and in any event no later than thirty (30) days from the conclusion of the Agreement.</p>
Authorised Sub-Processors	<p>For the purposes of this Agreement, the Processor is entitled to engage the following sub-processors, subject to complying with the requirements of the Agreement Part D clauses 1.11-1.12 and on the basis that data will only be processed within the UK:</p> <ol style="list-style-type: none"> 1. s31 / s43(2) 2. s31 / s43(2)

PART F

TENDER DOCUMENTS

1. DELIVERABLES

Specification

HM Government's National Cyber Security Strategy 2016 -2021¹ vision is that *the UK is secure and resilient to cyber threats, prosperous and confident in the digital world*. More recently the National Police Digital Strategy 2020 -2030² recognises that *Information is the lifeblood of policing therefore we must make the most of the masses of data made available to us enabling intelligence-led preventative policing and investigation, while continuing to meet citizen expectations regarding how we handle their data*.

Internet usage and cloud-based services, such as O365, are growing and the reliance on network data and devices is ever increasing. As legitimate network traffic increases so do the criminal opportunities. This has been highlighted with the COVID pandemic showing the advantages and risks an agile workforce working remotely can provide to a business or organisation.

Within policing there has been significant investment in the ability to fight cybercrime at a local, regional and national level with the creation of specially trained, dedicated cybercrime teams in every force and region working alongside the NCA's National Cybercrime Unit to pursue criminals who utilise computers and network infrastructure to commit crime.

Policing has adopted the '4P' approach to cybercrime breaking the focus into 4 main areas:

- *Pursue – to prosecute the individuals and criminal organisations causing the highest harm to the UK*
- *Protect – organisations and the community against cyber incidents*
- *Prepare – both policing and the community to defend and understand cyber incidents*
- *Prevent – prevent individuals becoming involved in cybercrime*

To enable law enforcement to target these areas an intelligence led approach is at the centre of the 4P model, but there is a gap in the intelligence we have. Talk to any cyber security

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

²<https://ict.police.uk/wp-content/uploads/2020/01/National-Policing-Digital-Strategy-2020-2030.pdf>
expert and they will say networks are under sustained attack from both global and UK based cyber threat actors. Policing recognises that it needs to address the changing pattern of criminal behaviour and offences. A large proportion of crime is now committed over the internet (both cyber-dependent and cyber-enabled). When compared with the physical world, the police currently have limited knowledge and intelligence about the criminal activity that is taking place online. As crime is increasingly committed in the cyber environment, both businesses and individuals are becoming more vulnerable to attack.

This is particularly so at the level of local policing and among micro to medium size enterprises³ who often lack the knowledge and funding to invest in cyber security. In a move to understand and address this risk and threat, policing is to offer to deploy technical measures that represent a new kind of police patrol and invite citizen engagement to create 'cyber neighbourhood patrols' which will enable a police vision to protect the cyber neighbourhood in partnership with local businesses.

It is imperative that these measures are lawful, proportionate and ethical. It is therefore necessary for any system procured to enable compliance with data protection, amongst other, legislation and for the supplier to engage constructively with the NPCC Cybercrime Programme's Legal and Data Protection Lead in connection with the initial and ongoing governance of the project, as well as to undergo scrutiny from that individual and the project's governance and ethics oversight committees. The system must enable the proportionate and secure collection, retention, destruction and processing of data only where necessary. Data processing must be logged and traced to enable auditing and the production of chains of custody in respect of data. The system must provide for alterations to ensure ongoing lawfulness and proportionality.

Project Pascal

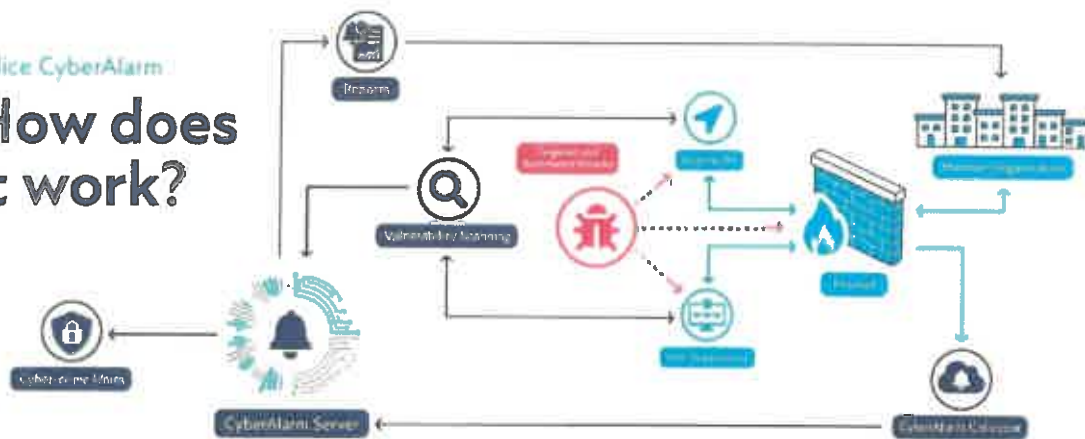
The NPCC Cybercrime Programme's 'Project Pascal' has been developing the ability for UK Policing to securely collect and analyse suspicious network traffic data. This is to enable law enforcement, working with industry partners, to better understand and respond to criminal attacks and allow for an improved understanding of the threats UK infrastructure faces on a daily basis with the overarching aim of: *"a capability to provide timely collection and processing of computer network traffic data to be able to analyse the data to produce information, intelligence and evidence in a legally compliant and ethical manner in order to Pursue, Protect, Prepare and Prevent."*

The initial focus of the project was perimeter suspicious activity data and vulnerabilities. This capability developed into Police CyberAlarm (cyberalarm.police.uk) which is currently available to all organisations and businesses but is focused primarily at SMEs. This does not preclude larger organisations from becoming members and supporting the wider community with their suspicious activity data even though they may have their own SOC.

³ For example, for Research and Development Tax Relief HMRC defines a SME as a business with less than 500 employees and either a turnover under €100 million or a balance sheet total of up to €86 million, but the more common definition of SME is defined by the Department for Business, Energy and Industrial Strategy (BEIS) and consistent with the EU definition (EU Recommendation 2003/361) of an SME:

- Micro Business = less than 10 employees and either a turnover under €2 million or a balance sheet total of up to €2 million.
- Small Business = less than 50 employees and either a turnover under €10 million or a balance sheet total of up to €10 million
- Medium Business = Less than 250 employees and either a turnover under €50 million or a balance sheet total of up to €43 million

How does it work?



The current system is focused in two area, suspicious inbound firewall data and vulnerability scanning of the member organisations external IP range and web applications. The data collected from multiple member organisations is the 'crowded sources' to enable law enforcement to better understand the strategic threat landscape and target 4P activity against the highest threat harm and risk. The member organisations also receive a number of reports:

- These reports allow the member organisation to better understand the current cyber threats against their organisation but also within their local area and industry sector. Enabling them to better inform and protect themselves against cyber-attack.**

Below is a snapshot of the level and types of data the current system is handling (Firewalldata and vulnerability scanning only) as of February 2021.

- Number of member organisations who have registered for access - 188
- Number of active Police CyberAlarm collectors - 40 (further 38 registered but not yet live)
- Average number of suspicious activity events per Police CyberAlarm member's collector 40,000 per month
- Number of vulnerability scan targets live in the system – 18
- Number of vulnerability scans completed – 162

New System

Following on from the initial success of Police CyberAlarm, the NPCC Cybercrime Programme is looking to procure the next iteration of the Police CyberAlarm system. This will increase the number of data types the system can handle including cloud-based data points, improved functionality and usability along with the ability to commercialise aspects of the system to help support its wider rollout and sustainability.

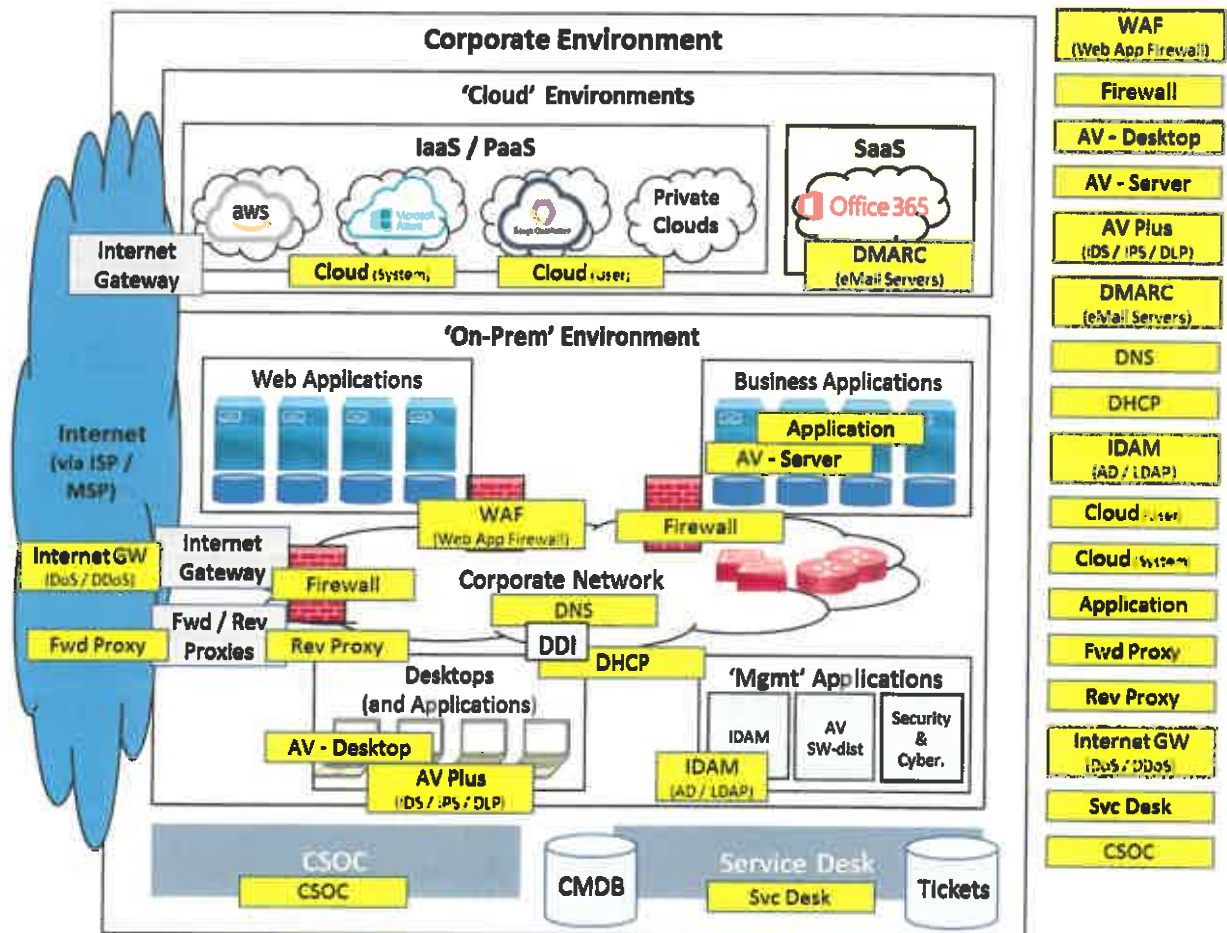
The new system needs to take the existing functionality within Police CyberAlarm including:

- The ability to ingest Firewall logs
- The ability to enrich and categorise Firewall logs
- The ability to analyse events and correlation of events of interest through standard reporting and ad hoc analysis
- The ability to vulnerability scan the external IP addresses, external websites and endpoints of a member organisation for known vulnerabilities
- Regular automated reporting to member organisation

As part of the ongoing development of the existing system and research, further data end points have been identified as providing a potentially rich intelligence source for policing. These include:

- The ability to ingest and analyse IDS/IPS log
- The ability to ingest and analyse email and IM SPAM logs from central collection points rather than individual end points.
- The ability to ingest and analyse network AV logs

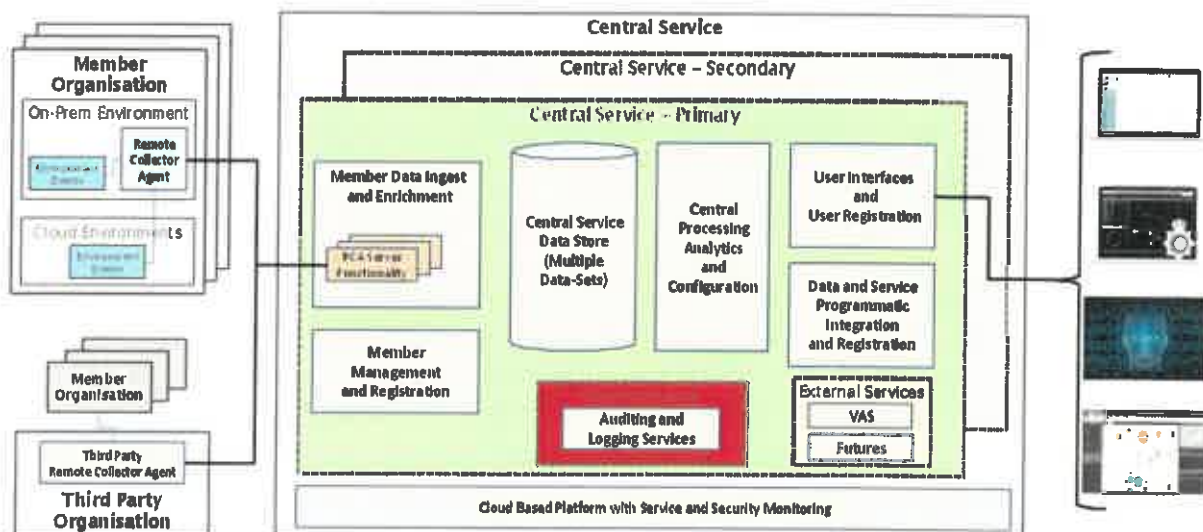
The system will also need to be able to ingest the cloud-based variants of these data types from IaaS, PaaS and SaaS environments and have the ability to easily include additional on-premises and cloud-based data types in the future. The diagram below is indicative of the data types that could be considered for inclusion in the system as it expands.



NOTE: Every Environment will be slightly different, but these are indicative of the types of logs that are generally available within corporate environments

System Topology

The below diagram outlines the potential overarching system topology of your solution.



System Scale and Commercialisation

Due to the 43 force model in England & Wales along with the regional and national policing structures throughout the UK, the system will need to allow for different levels of access

between the different legal entities horizontally but also between the different levels of investigation: local, regional and national.

The system will need to be fully scalable with the ability to grow as the membership base grows and scale up and down dynamically to membership data ingest throughput volumes. Ideally, this will be utilising cloud technology to allow for both vertical and horizontal scaling for membership and efficiency in processing and data storage costs.

Although the current system is free at the point of delivery to members, consideration needs to be given to the long-term sustainability of the system. Consideration needs to be given within the procurement to allow for the system to have a tiered pricing model with a cost being attached to extra services; there may also be the option of sponsorship or the ethical commercialisation of the collected and/or enriched data. All of these options would be to support the wider and continued rollout of the system.

Member Organisation Registration

The system will need to be simple to both register as a member and to install on the members' network or cloud-based infrastructure. The system will also need to be able to interface with the various different makes and models of security device within a member's network with a minimal footprint both in size and processing used.

The management of this membership will also need to be simple with the ability to manage members based on their geographical location within the UK and potentially a level of member self-service to enable for example the live viewing of suspicious activity, data, reports and updating of registration details.

The member organisation registration process will need to be simple to allow for organisations with limited computing skills to both register and install the relevant collection devices on the network. There will need to be clear instructions as to the process along with remote technical support for those organisations that are unable to install the collector.

An approval and auditing process needs to be built into the registration to allow forces to understand and approve who is requesting access to the system and monitor their progress. The process will also need to include the ability to digitally sign and approve the terms and conditions of access and data sharing.

Police User Registration

The system will need to be able to authenticate the police users of the system via a web-based portal. Authentication will need to be a minimum of 2FA and be limited to specific email domains including pnn. When registering the users on the system extra data will need to be collected including but not limited to Force, ID Number and Rank.

Data Acquisition

'Suspicious activity data' is any activity across the four data elements (Antivirus, Intrusion Detection/Prevention, Spam logs and external traffic logs), recorded by the member organisations' networks logging systems as suspicious, linked to an attack or part of an attack, i.e., denied traffic and which is confirmed to fall within the definition of suspicious by the Police CyberAlarm system.

In respect of each of these 4 data elements, data will need to be first identified as 'suspicious' by the member organisation themselves, by their firewall, antivirus and spam detection software. All of this data will need to be verified by being subjected to a collection filter, which applies rules to the collected data to prevent the inadvertent further processing of data that cannot properly be identified as 'suspicious', internal to external data, for example.

Only the log data of the traffic/communication identified as suspicious activity should be captured or shared with the Police, although this may include header data such as the subjectmatter of a communication. The suspicious activity data will be analysed, and any false positive logs identified and destroyed. Confirmed suspicious activity logs will be retained for a specified period of time currently 9 months and then destroyed unless it is identified as being correlated to further suspicious activity. If correlating suspicious activity data is obtained within a 9-month period then the data would be retained for 9 months from the last correlating data, unless the data is extracted onto a police system as part of an investigation in which case it would be treated in accordance with the Management of Police Information (MOPI) principles⁴.

The combined 'crowd sourced' data collected from all the member organisations must then be capable of being analysed in real time to highlight any useful intelligence from either a single or multiple organisations, identifying cyber-attacks and cybercrime trends. The member organisation must be sent automatically generated periodic reports from Police CyberAlarm alerting them to attacks they have had should they wish, as well as wider intelligence and data capable of highlighting any potential issues in their firewall or cyber security set up.

Central Processing

The system will need to have a number of built-in analytical functions to enable exploitation of the data received from member organisations either at a force, regional or national level. These will need to be accompanied by a confidence score as to the accuracy of the data where appropriate. The system also needs to allow for the data to be analysed to show trends in frequency and types of attacks against a region or industry sector. The system needs to be user friendly allowing non-analytically trained staff to understand the results. Although useful on its own, the police need the capability to enrich this data with other closed and open-source data sets to allow for its full value to be gained.

The use of such data sets provides the opportunity, for example, to attribute the geolocation of a data subject's IP address to a region or country (for example this could be indicated using `inetnum`/`inet6num` object data), provide access to the IP registrant's details, or allow comparing against known bad IP addresses (that is addresses previously identified as being involved in criminality by either industry or law enforcement agencies). Where the analysis of the data against data sets takes place, with the consequence that a value is attributed to the data, such as where suspected geolocation is attributed to an IP address, this is likely to be based on numerous data sets and must identify the dataset(s) used and be marked as being subject to a confidence score as to the likelihood of this being correct. In the event that any such data is extracted or shared, this score will also need to be capable of being included with the extracted/shared data.

The system will need to permit the extraction of data via an ETL mechanism or API to enable further analytics and data enrichment using other software solutions, for example Maltego (an open-source intelligence (OSINT) and graphical link analysis tool for gathering and connecting information for investigative tasks, which enables integration of data sets from a range of partner organisations), Elastic Stack (a distributed, RESTful search and analytics

<https://www.app.college.police.uk/app-content/information-management/management-of-police-information/>

engine which centrally stores data), or Kibana (an open-source data visualization dashboard for Elastic search).

System Security and Testing

The expectation is that the system will need some form of software installed within the member organisation's network infrastructure both physical and cloud. This in itself presents a potential risk and attack vector to the member organisations. The system will need to be available for regular penetration testing and code review by external qualified partners and any remedial work promptly actioned.

Police CyberAlarm (Pervade) Collector Transition

The current Police CyberAlarm system has been available since September 2020 and has a growing membership. These members will need to be migrated over to the new system (including decommissioning the current collectors and integrating the new remote collector agents) alongside the installation for new members. This transition will need to be conducted with minimal intrusion on the member organisations day to day business with minimal loss of service to them. All current members will need to be migrated to the new system by 31st October 2021.

Police CyberAlarm (Pervade) Data Migration

Consideration will need to be given to migrating the current Police CyberAlarm's data set over to the new system to create a single data set. API or ETL access will be granted to allow for this data to be ingested by the new system, if appropriate.

Full details will be provided to the successful supplier who will work with the incumbent supplier to successfully migrate data within the agreed timeframe.

Phased Rollout and Implementation

As outlined in the Technical Specification the rollout of Police CyberAlarm will be split into two Phases:

Phase 1 – initial rollout of the system to current and new members focusing on maintaining and migrating the current system data, members and capability to the new service. The intention is for this to have minimum impact on the current members.

Phase 2 - Introduction of enhanced data types including IDS, AV and Spam along with scoping and possibly introducing the ability to charge for extra services, for example live time reporting of cyber incidents, or other funding streams to assist in the maintenance and growth of the system.

a) Tender Response (ITT Submission)

General Architectural Overview	
Context: To correctly set the context of your proposed solution, it's useful to have an overview of your end-to-end architecture.	
Question 4.1	<p>Please provide a high-level architectural overview of your proposed end to end solution and service, clearly indicating any specific technologies, including the use of open-source components, that will be able to fully meet the requirements of the programme.</p>

s31 / s41 / s43(2)

s31 / s41 / s43(2)

s31 / s41 / s43(2)

Member Registration:

Context: Members are required to register with the Central Service before they can install Remote Connector Agents. This process must be initiated and managed by Police users and include registering basic details about the member organisation, validated against industry standard meta-data, and specific details about their location(s), IT environments, data types available and Remote Connector Agent(s) to be deployed. These can then be downloaded and integrated into the members IT environment. After the initial registration and activation, membership details and configuration must be maintained and updated when additional data types become available from the member or other circumstances change. It is also possible that Third Parties could be used to provide data about members, and would require a similar registration and management process. In the future it may be required for the central service to collect payments from member organisations for enhanced services, which will require different additional registration details to be captured and maintained.

Bidder Response**Question
4.2**

Please provide details of how your solution handles member initial registration and ongoing management, including details of any automated features that can demonstrate more efficient ways of working and directly benefit Police resource effort

s31 / s41 / s43(2)

s31 / s41 / s43(2)

**Question
4.3**

Please provide details of how your solution would manage third party registrations

**Question
4.4**

Please describe how your solution could handle payment registration, collections and account management in the future if required?

Member Data Ingest:

Context: The central system must be capable of collecting data from members on-prem and cloud based environments via one or more Remote Collector Agents or Third Party Remote Collector Agents in a secure, resilient and dynamically scalable way, storing a copy of this source data within the central system.

The Initial data types collected must include Firewall logs, IDS/IPS logs, Anti-Virus logs and email SPAM logs, but the system should not be limited to these data types and must be easily configurable to collect additional data types from the members on-prem and cloud based environment, within the agreed parameters of the Data Handling Schedules.

It is expected that different 'protocols' and transport types will be available from the Remote Collector Agents and Third Party Remote Collector Agents, and these will all provide secure, resilient and dynamic scalability into the central service to optimise compute and storage needs. There is the possibility that any data collected could be used as part of criminal prosecution. All data collected will need to be able to show its 'chain of custody' and that it has not been altered since being ingested into the system.

Bidder Response

**Question
4.5**

Please provide details of how the central service of your solution will collect the data types identified above in a secure, resilient and scalable way, including details of the 'protocols' and transport types supported?
NOTE: Questions related to Member specific integration of RCA/TP-RCA are covered in the section below.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

s31 / s41 / s43(2)

**Question
4.6**

Please provide details of how your central service solution could collect potential future data types in a secure, resilient and scalable way, and how the requirements of the proposed Data Handling Schedule would be implemented in connection with this?

**Question
4.7**

Please describe how your system will ensure, through logging and system controls for example, that a chain of custody is created and maintained in respect of each item of data, and any processing that has been undertaken in respect of it, to ensure that data could be used in evidence if necessary?

Member Data Enrichment:

Context: It is important to enrich data received into the central system in a timely manner, including adding any extra details / tags about the source of the data that could be useful for subsequent analysis and processing. This could include adding any geolocation details or IP / Other Indicators of Interest that are associated with source data at the time it enters the PCA system. It could also include tagging information to the data records about the member organisation it originates from, such as their Industry type.

Bidder Response

**Question
4.8**

Please identify each of the data enrichment options available from your solution, where the enrichment data is obtained from and how its use complies with data protection legislation (particularly, but not exclusively, the source(s) of enrichment data, the accuracy of the data, any data transfers, the legal grounds for processing and the transparency measures in place). If 3rd party data enrichment products are used please confirm product and version details, any restrictions on the use of the enriched data source, and any pricing implications from its use.

s31 / s41 / s43(2)

Question 4.9 If your solution also transforms the ingested and enriched data records into a common format, please provide details of these formats and transformation rules.

s31 / s41 / s43(2)

Member Self-Serve Portal:

Context: After Members Initial registration additional details are required that need to be maintained, and members will receive regular reports via email. This capability could be provided by a Members self-service portal and offer functionality such as:

- Ability to update key member attributes and regularly confirm accuracy
- Provide an internal dashboard of member specific suspicious activity in a easily reviewable and understandable format
- Ability to review and download PDF reports instead of them being emailed
- Ability for the member to see, and potentially alter, the reporting schedule used to generate these reports, including confirmation of any cost implications.
- Reports should be able to be generated weekly or monthly and present all data for the reporting period
- ability of the central system to inform member organisations of live suspicious activity

Bidder Response

Question 4.10 Please describe how Member Organisations are able to update their details following registration.

s31 / s41 / s43(2)

Question 4.11 Please provide details of how you would add value to the system to allow for 'enhanced services' which could be charged for?

s31 / s41 / s43(2)

SECURITY RELATED:

Data Handling Legal Framework:

Context: The Central Service must comply with the Data Protection Act 2018 (including as applicable to law enforcement processing), the GDPR, the Law Enforcement Directive, and meet ethical requirements, from Initial collection of data from members, third parties and the public domain, to the processing, analysis, storage and destruction of data. This will be required for the initial data types and, where necessary, will be updated and maintained when additional data types and controls are added in the future. This necessitates: appropriate access controls; auditing measures; technical and organisational security measures; confidentiality obligations imposed on staff; staff data protection training; data minimisation; data logging; appropriate transparency; legal grounds for processing (particularly in collection with the gathering and deployment of third party datasets and analytical tools); ethical machine learning and artificial intelligence, and support for related governance; the ability to identify the data controller on whose behalf data is collected; the ability to support the conduct of DPIAs and the response to regulatory and data subject enquiries and rights requests; data breach mitigation and incident response

Bidder Response

procedures, etc.

**Question
4.12**

The system will need to be accredited by NPIRMT and NPCC and signed off by key stakeholders, such as DPOs, SIROs, etc at F-R-N levels. Please describe how your solution will meet these requirements, and how you will work with NPCC to proactively maintain them throughout the lifetime of the contract?

s31 / s41 / s43(2)

Security Classification:

<p>Context: The central service should be accredited to Official-Sensitive and appropriate accreditation document sets, such as Information Security Management System (ISMS) assessments and Risk Management and Accreditation Document Set (RMADS), etc) must be maintained.</p>	
<p>Question 4.13</p>	<p>Please describe how your solution will meet this level of security classification and your approach, processes and procedures to maintain this level of accreditation? Please indicate any requirements you may have on NPCC to support and maintain this accreditation.</p> <p>Bidder Response</p> <p>s31 / s41 / s43(2)</p>
<p>Audit and Logging requirements:</p> <p>Context: All operations within the Central Service must be logged, including but not limited to:</p> <ul style="list-style-type: none"> - All user Create, Read, Update and Delete (CRUD) operations for data access, query or analytics operations, report generation, data copying, etc - All Administrators CRUD operations - All API / Programmatic CRUD operations - All configuration or rule changes - All 'meta-data' updates - All System and 3rd part component 'upgrades' <p>All logging should include consistent and accurate timestamps (UTC with Time Zone) and should be written to a separate, isolated, secure central audit area, and all data should be maintained for system defined retention periods, although it is expected a tiered access time approach would be adopted to minimise cost implications.</p> <p>Question 4.14</p> <p>Please confirm the auditing and logging capabilities of your solution, including compliance with the requirements above and any potential gaps?</p>	
	<p>Bidder Response</p> <p>s31 / s41 / s43(2)</p>

Question 4.14	Please confirm timestamps and accuracy to be used, and any potential concerns or implications?
Question 4.15	Please address any options and implications for a tiered storage solution for this type of data?

System Security Model:

Context: The Police follow a Force / Regional / National (FRN) model with Forces providing resources and being responsible for public interaction and data obtained from members within their geographical area. Regional and National levels provide additional expertise to support forces and focus on organised crime which often crosses multiple force areas.

The system should have a flexible security model to support this FRN model and ensure force users can only see data from their area, regional users can see data from all forces within their region, and national users have access to all data available.

However, the FRN model isn't always aligned to member organisations structures so the central service security model must allow member organisation 'views' to be defined and provide granular access controls to members data which may be across multiple force areas.

Additionally, some analytical services may also require this granular access to multiple forces data.

It is envisioned that the central system will have a 'super admin' that has access to all areas and is strongly protected but rarely used. It must be possible to create

Bidder Response

other admin roles for users, data, service and system controls within the FRN model and enable granular access for specific tasks and users.

**Question
4.16**

Please describe how your system security model will meet these FRN and member requirements for users, data and services including capabilities for specific granular access controls?

s31 / s41 / s43(2)

s31 / s41 / s43(2)

CENTRAL PROCESSING / CAPABILITY RELATED:

Central Processing - Real-Time Analytics:

Context: The system must be able to inspect the enriched data ingested from members and third parties, and automatically detect and categorise any potentially suspicious activity based on the type of records and time sequence. This could include grouping records that indicate a specific suspicious activity, such as port scan reconnaissance

The system should also be able to detect sequences of suspicious activity against a specific member, such as port scan reconnaissance followed by access attempts, or combinations of multiple events from different data types, such as suspicious email and IP events from the same source.

In addition to identifying suspicious activity against individual members, the system should also detect any correlations of similar activity across multiple members at FRN levels, and indicate any specific characteristics such as an attack on common industry types or from a common source.

The system should also highlight the potential seriousness of the activity and the probability of being able to resolve it to help the Police prioritise the type of action to be taken.

Bidder Response

**Question
4.17**

Please describe how your solution will meet and extend the real-time analytics requirements identified above, including details of additional scenarios, data or analysis that you consider relevant.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

s31 / s41 / s43(2)

**Question
4.18**

Please describe any characteristics or techniques you would use within the User Interface to ensure this results data is readily available and 'Police User Friendly'.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

Question 4.19	Please confirm the range of these capabilities available through the Programmatic Interface.
---------------	--

Central Processing - Enhanced Analytics:

Context: In addition to the real-time analytics the system should have the capability to perform enhanced analytics and deeper analysis of broader data sets at FRN levels and identify other potentially suspicious activity or broader correlations of events over a longer timescale. This could then be used to optimise the real-time analytics or for other purposes.

It could also be useful for other tools or granular DevOps components to be available for this purpose and have access to the broader data sets but work within the system security model and don't compromise the integrity or availability of the operational service.

Question 4.20	Please provide details of the range of enhanced analytics available within your service, the range of options for supporting other products or components, and the implications on the User Interface?
---------------	--

Bidder Response

s31 / s41 / s43(2)

s31 / s41 / s43(2)

**Question
4.21**

Please describe any operational and commercial implications of using enhanced analytics, and options for ensuring value for money.

s31 / s41 / s43(2)

Central Processing - Analytics configuration:

Context: The central service should come with many pre-configured 'rules' for identifying and categorising suspicious activity, and it must be possible to easily maintain and extend these. A full audit trail of all config changes must be maintained to ensure any retrospective investigations will know exactly what configuration 'rules' and versions were applied to data analysis at the time. All 'Rules', or other techniques, must be configured system wide (effectively National level) and can only be configured by appropriately authorised users. A full audit trail must also be maintained for Enhanced Analytics, but the specific implementation details may be slightly different.

Bidder Response

**Questions
4.22**

Please describe the range of pre-configured rules available within your core central service solution.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

**Question
4.23**

Please describe the range and flexibility of configuring additional rules and controls into this solution, including testing and deployment controls.

s31 / s41 / s43(2)

Question 4.24	Please describe how Enhanced Analytics configuration and auditing is maintained.
----------------------	--

External Services:

Context: The PCA system must be able to provide External services to members, such as a Vulnerability Analytics service.

These services will need to be configured within the central service at a FRN level, scheduled to run against a members environment or a subset of their environment (i.e. not a full scan every time), and the results returned to the central service where they can be combined with other information relevant to the member and produce a report.

The External Service should operate from a separate area that cannot compromise the PCA central service, and should be flexible enough to support a broad range of external services, some of which may be chargeable.

Question 4.25	Please provide details of how external services can be integrated into PCA, scheduled to run against members environments, and how the results can be combined with other data to produce member specific reports. Please explain any other features or safeguards you think could add value to this service, and how any charging would be administered.
----------------------	--

Bidder Response

s31 / s41 / s43(2)

s31 / s41 / s43(2)

Future Innovation:

Context: The cyber threat to members will continue to evolve so it's important that this service is able to maintain and enhance its relevance to member organisations and continue to provide valuable threat and trend intelligence to Policing.

There are many emerging technologies and products that could benefit this type of service, including but not limited to:

- Integration with other data sets (Dark Web, etc)
- SOAR (Security Orchestration, Automation and Response)
- AI/ML (Artificial Intelligence / Machine Learning)
- Increased computing and analytical capabilities through specialist hardware (GPU, FGA, etc) and Quantum computing
- etc

It is also expected that processes and procedures will continue to evolve and improve, and any emerging techniques that increase efficiency should also be incorporated into this service.

Bidder Response

**Question
4.26**

Please describe your approach to innovation and how it would be incorporated into this service, including addressing any commercial or IPR considerations and how you would approach any changes to the current legal framework that may be required.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

Law Enforcement - USER INTERFACE RELATED:

User Interface - Look and Feel

Context: The solution should provide an intuitive police friendly user interface accessible via a secure web-based portal and be scalable within resizable windows. It should provide the ability to visualise and interact with data and analytical processes and support multiple styles to reflect different analytical views, such as highlighting attack locations on maps, showing sequences in pipelines, etc
The capability available within the User Interface will be determined by the users' permissions and features should not be presented that are not available. This could range from broader areas, such as administrator screens only being available to admin users, through to specific analytical tasks only being available to certain users or user roles.

Individual users will be able to customise and personalise

Bidder Response

their user interface (and reportings) to meet their specific requirements, and subject to appropriate security permissions users should have the option to download reports and data sets from within the Browser

**Question
4.27**

Please confirm how your product will support these requirements, providing examples of police friendly UI where possible, and suggest any additional or alternative features that you consider relevant based on your experiences of implementing your solution.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

**Question
4.28**

Please confirm the range of browsers (i.e., Edge, IE, etc) and platforms (i.e., Windows, etc) supported and any additional components (plug-ins) or configuration required?

s31 / s41 / s43(2)

NOTE support for Mobile devices or small screen formats is not required.

s31 / s41 / s43(2)

User Interface - User Registration and Authentication

Context: All users need to be Registered with the PCA system and successfully authenticated through the user interface before being granted access to the data and services they are permitted to use.

The initial registration must be completed by an appropriate administrator following the FRN system security model. The User ID must be a valid email address from a centrally configured limited number of email domains. These will mainly be PNN email IDs but could also include other law enforcement and government partners. Passwords will be specific to PCA and comply with PCA password policy.

Following initial registration, the user must be able to add additional details private to them that can be used through a self-service user portal for tasks such as changing passwords or resetting forgotten passwords, etc. User authentication should also include 2 Factor Authentication, although Single Sign On is not required. There are many approaches and standards available for Password and user details Storage and Policy and these can evolve overtime.

Bidder Response

**Question
4.29**

Please describe the options and your recommendations for user registration, management and authentication within your solution, including its capabilities for storing and managing passwords and enforcing password policies.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

CENTRAL HOSTING RELATED:

Central Service Hosting Environment:

Context: The Central Service should follow the UK Government 'Cloud First Policy' and be compliant with a number of international and UK standards and best practices, such as:

- ISO 27001
- Other ISO Standards, such as ISO 27017 / ISO 27018 / ISO 27032
- NCSC Cloud Security Guidance
- NPIRMT PASF accreditation of data centres.
- Cyber Essentials / Cyber Essentials Plus.

All data must reside and be contained within the UK and should not be visible to other cloud users or cloud services.

Bidder Response

**Question
4.30**

Please confirm the details and compliance levels of your proposed hosting solution for the central service.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

Central Service Resilience and Scalability:

Context: The Central Service should be able to exploit cloud platform services for all operations, such as:

- Elastic scalability and load balancing of Compute and Network resource
- High levels of resilience across multiple hosting centres within the UK
- Cost effective use of Intense compute operations
- Effective use and management of storage and archive tiering
- Exploit Cloud Platform Database services where appropriate
- Utilise Cloud Platform Serverless services where appropriate

Bidder Response

s31 / s41 / s43(2)

**Question
4.31**

Explain how your solution can exploit these, and other, capabilities and provide a cost effective, resilient, secure and scalable solution for the central service.

**Question
4.32**

As the cost of cloud services will be 'pass-through' please evidence how you will proactively monitor and manage these costs to ensure best value for money.

Central Service Security Configuration options:

Context: The Central Service should encrypt all data in transit and at rest (including replicas and backups / archives) and ensure this is maintained when using cloud-based services.

Bidder Response

**Question
4.33**

Please confirm the security capabilities of your solution, including any potential concerns and describe any options for key management.

s31 / s41 / s43(2)

Central Service Monitoring:

Context: The Central Service must be proactively managed in real-time to ensure efficient and cost-effective operations and must contain active cyber security defences and controls to proactively monitor, detect and block Malware, DLP, Viruses, etc that may have got onto the central service and isolate any impacted service without impacting the overall service.
It is also expected that regular internal vulnerability assessments and external pen tests will be conducted on the central service.

**Question
4.34**

Please explain how your solution will meet these System and Security monitoring requirements and include any additional measures you deem appropriate, and also provide details of how any incidents will be managed and mitigated.

Bidder Response

s31 / s41 / s43(2)

s31 / s41 / s43(2)

DATA INTEGRATION / EXTRACTION RELATED:

Data and Service Integration:

Context: The central service must be able to make its data and business logic immediately available for external use in an industry standard common format / structure and enable recursive bulk extraction at speed for use by custom User Interfaces and external analytical tools such as Maltego.

The potential interfacing options could include:

- APIs to access business logic and data, returning zero, one or multiple data sets.
- ETL capability to recursively extract larger volumes of data from the central system
- SQL Access to data and embedded business logic

All interface options should maintain the integrity of the

Bidder Response

central service and adhere to the system security model and auditing and logging standards.

**Questions
4.35**

Please provide details of the types of Interfaces, options and standards available within your product / service including:

- the range of capabilities enabled (i.e. RO or CRUD) and details of return codes and exception handling.
- the scope of data and business logic available to them (i.e. small subset of data, or full access to all data and logic).
- Interface option specific security controls.

NOTE: If helpful in explaining this capability links to existing product documentation will be acceptable and won't be included within word count of the response.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

Data and Service Integration Registration:

<p>Context: All external programmatic access must be via an authentication mechanism which relates to a unique system identity than can be configured with appropriate access controls and complies with the central system security model.</p> <p>The central system must have an appropriate system user admin area linked to the FRN model that is able to create programmatic access 'tokens'.</p> <p>There are options for providing programmatic authentication 'tokens', but they should have defined validity periods and it must be possible to revoke them before this validity period expires. There should also be management processes in place to renew before expiry, if appropriate.</p>	<p>Bidder Response</p>
<p>Question 4.36</p>	<p>Please provide details of the programmatic authentication mechanisms supported by your solution for all external interface types.</p> <p>s31 / s41 / s43(2)</p>
<p>Question 4.37</p>	<p>Please provide details of the user interface for programmatic access management, and any associated management processes.</p>

s31 / s41 / s43(2)

GENERAL DEVELOPMENT APPROACH RELATED:

Development Standards:

Context: This system will be a high-profile Police branded national system, so it's imperative that strong SDLC practices are followed that would satisfy external scrutiny

Bidder Response

**Questions
4.38**

Please describe your approach to SDLC standards and methodologies, build and testing approaches, processes and tools, and broader Enterprise Quality Assurance processes and accreditations that you will utilise when delivering this product or service capability.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

s31 / s41 / s43(2)

Technical - Remote Collector Agents

RCA Coverage:

Context: The RCA clients are installed within a member's environment and integrate with the RCA Server in the Central Service, but members environments vary considerably and will have different vendors products to meet their network and security needs in their on-prem and cloud-based environments. To maximise potential member coverage, it's important this service has a broad range of supported RCA clients available, and options for integrated 'non-standard' environments.

Bidder Response

Question 4.39

Please provide details of the range of RCAs you provide and support, including generic syslog and file RCAs through to details of specific network and security vendors devices (including supported versions) and any vendor specific enhanced integration protocols that are supported (such as Cisco eStreamer).

s31 / s41 / s43(2)

s31 / s41 / s43(2)

s31 / s41 / s43(2)

Question 4.40	Please provide clear details about how your RCAs integrate into IaaS / PaaS Cloud based environments, such as AWS, Azure, GCP, etc, and SaaS based environments such as O365 and other popular business applications.
Question 4.41	Please provide details of how you would integrate environments without currently supported RCAs.
Question 4.42	Please describe any additional details or considerations to enable your RCAs to work within a Third-Party environment, such as an MSP or ISP.

s31 / s41 / s43(2)

RCA Member Integration:

Context: When a member has been successfully registered and additional details of their IT environment have been collected, they will be able to install one or more RCAs into their on-prem and cloud-based environment and will be sent appropriate installation instructions.

Bidder Response

**Question
4.43**

Please detail your approach and experiences of installing and maintaining RCAs within member environments, including the level and type of support required (none / remote / onsite) and 'typical' installation and configuration times? Please include any particularly complex scenarios you've encountered, and how you've integrated members environments that don't have supported devices.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

**Question
4.44**

Please confirm how the RCAs will collect the initial data types required (Firewall logs, IDS/IPS logs, Anti-Virus logs and email SPAM logs) and how they can be extended to include additional data types in the future.Aa

s31 / s41 / s43(2)

Question 4.45	Please provide details of Physical / Virtual device requirements and any other Installation guidelines required to support RCAs within members environments, clearly identifying any performance, resilience and security considerations.

RCA Security and maintenance:

Context: It's vital that the RCA client does not introduce any security risks into the members environment and the RCA client / server protocol is secure and resilient. It's also necessary to be able to manage and maintain the RCAs installed within a member's IT environment with no (or little) impact on the service or support from members.

Bidder Response

Question 4.46 Please describe how RCAs are installed within members IT environments and any specific guidelines and principles that must be followed to ensure no potential security compromises are introduced? please include any additional guidance applicable to Third Party TP-RCA environments.

There are 2 ways to install a Remote Data Collector either as a

s31 / s41 / s43(2)

s31 / s41 / s43(2)

Question 4.47	Please provide details of your RCA client / server protocol, including and security and compression algorithms used, and any differences between the different types of RCAs.
Question 4.48	If your RCAs persist any data locally within the members IT environment, please provide details of security and encryption controls applied to this data.

Question 4.49	Please confirm the capabilities of your solution for RCA management and maintenance, including config updates, patching, disabling, certificate / token management, etc.
----------------------	--

s31 / s41 / s43(2)

RCA existing installations:

Context: In order to increase the coverage and number of members, it could be beneficial to integrate any existing customers you have for your product into PCA.

Bidder Response

Question 4.50	Please describe the viability of leveraging existing product installations to also support PCA, including any commercial, contractual or data handling implications and a technical overview of how this could be achieved.
----------------------	---

s31 / s41 / s43(2)

RCA existing PCA Migrations:

Context: The current PCA system has been deployed to multiple members that will need to be migrated to the new PCA system.

Bidder Response

**Questions
4.51**

Please describe your approach to migrating existing customer installed bases to your solution, including likely timescales and challenges and include mitigations and examples where possible.

s31 / s41 / s43(2)

Vulnerability Analytics

External Services Integration:

Context: The PCA central service has the capability to integrate many external services and provide a consistent approach for PCA users to schedule and execute these services, providing the external service with member specific parameters (such as Public IP addresses), and combine the results from the external services with other PCA data relevant to the member and produce enhanced member specific reports.

The central service may also allow members to request external services through a member portal and will handle any commercial implications for executing external services.

Bidder Response

**Question
4.52**

Please define the generic architecture and how you will integrate external services into the central service.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

s31 / s41 / s43(2)

External Services Vulnerability Specific:

Context: The scanner should be a recognised scanner that provides results using standard CVE codes, severity and common vulnerability names and at a minimum software should be able to test for:

- SQL Injection
- Cross-Site Scripting (XSS)
- Remote command execution
- Authentication Bypass
- Common file brute force
- Software identification

Bidder Response

**Question
4.53**

Please confirm the capabilities of your Vulnerability Analytics service and the technology it's built upon, the meta-data and signatures it uses and options for controlling the depth / intrusiveness of specific scans and ability to focus just in parts of the members IT environment.

s31 / s41 / s43(2)

s31 / s41 / s43(2)

Question 4.54	Please confirm what safeguards are in place to ensure the members IT environment being tested doesn't believe it's under attack and initiate its own actions, and please confirm how you would respond to any such unintended consequences.
Question 4.55	Please identify any specific differences or constraints for cloud-based IaaS and SaaS solutions.

b) Bidder Response Clarifications

s31 / s41 / s43(2)

s31 / s41 / s43(2)

2.

COMMERCIALS

a. Pricing Model

s41 / s43(2)

s41 / s43(2)

FOIA Restrictions

Without limitation, the pricing model detailed in this Part, is provided in confidence by the Service Provider and is considered to be commercially sensitive. Furthermore, and again without limitation, the Background IPR of the Service Provider is similarly commercially sensitive and may be confidential.

CHANGE CONTROL NOTICE [No.]

PO Number: [INSERT]

PART G

CHANGE

REQUEST

Requested By:	
Date Requested:	
Description of Change:	
Reason for Change (full description):	
Details of any proposed alternatives:	
Benefits and disadvantages of requested change:	
Implications of No Action:	
Priority (High = immediate attention required, Medium = schedule with next available iteration, Low = address when most economical)	

Signed by Requester: _____

Date: _____

CHANGE AUTHORISATION

Detailed description of change and Impact assessment:	
Proposed adjustment to the Charges resulting from the change	
Cost breakdown:	
Intended date for change:	

Signed by CUSTOMER: _____

Name: _____

Position: _____

Date: _____

Signed by SERVICE PROVIDER: _____

Name: _____

Position: _____

Date: _____

PART H

**[PRINT ON SERVICE PROVIDER'S COMPANY
HEADED PAPER]**

CERTIFICATE OF DECLARATION

PO Number [INSERT]

We, Pervade Software Ltd, certify that ALL of the following:

1. the Customer's Confidential Information under its control or in its possession;
2. the Customer Data, or media containing the Customer Data or other materials provided by the Customer; and
3. the Customer owned property in the possession or control of the Service Provider, to the Customer;

have been returned, destroyed or deleted in accordance with the Agreement dated _____.

Signed by

Board Director [SERVICE PROVIDER]

Date

PART I CONTACTS LIST

**KEY PERSONNEL
SERVICE PROVIDER**

NAME	TITLE/JOB DESCRIPTION	CONTACT DETAILS
s40(2)	CTO	s40(2)

OTHER CONTACTS (NON-KEY PERSONNEL)

SERVICE PROVIDER

NAME	TITLE/JOB DESCRIPTION	CONTACT DETAILS
s40(2)	Managing Director	s40(2)
	Senior Systems Engineer (Programme Roll-out)	
	Help Desk Support	

CUSTOMER

NAME	TITLE/JOB DESCRIPTION	CONTACT DETAILS
s40(2)	Project Lead	s40(2)
	National Co-ordinator	
	National Cybercrime Programme Lead	

PART J SPECIAL TERMS

SPECIAL TERM	EFFECT OF SPECIAL TERM	CONTRACT PART	CONTRACT CLAUSE	REVISED WORDING
1.	Amends existing clause	Part A	2.1.1	The Service Provider acknowledges that It: has made and shall make its own enquiries to satisfy itself as to the accuracy and adequacy of any information supplied to it by or on behalf of the Customer or any other Service Recipient;
2.	Inserts additional clause	Part A	5.5	The Service Provider shall enter into such further contracts or agreements as are necessary to give effect to the terms of this Agreement including, without limitation, prior to processing any Personal Data on behalf of a Service Recipient, the Service Provider and Service Recipient shall enter into a contract in the terms set out at Part K, which the Parties acknowledge and accept is necessary to give effect to the terms of the Agreement.
3.	Amends existing clause	Part A	Clause 8.1	The Service Provider shall provide the Support Services in Part B following each Go-Live to the Customer and Service Recipients.
4.	Amends existing clause	Part A	Clause 9.5	<p>9.5 The Service Provider shall:</p> <p>9.5.1 invoice the Customer for the Charges during the Initial Term s43(2)</p> <p>s43(2)</p> <p>9.5.2 apply any payments made by the Customer during the Initial Term which exceed the Charges to any Subsequent Term or, if no Subsequent Term is entered into, refund those payments to the Customer within thirty (30) days of the expiry of the Initial Term;</p> <p>9.5.3 be entitled to payment of any Charges in excess of the payments made by the Customer during the Initial Term under clause 9.5.1 above within thirty (30) days of supplying the Customer with a compliant Invoice following the expiry of the Initial Term;</p> <p>9.5.4 in respect of any Subsequent Term, and subject to any reduction to the Charges having regard to clause 9.5.2 above or clause 9.5.5 below, Invoice the Customer s43(2)</p> <p>s43(2)</p> <p>Subsequent Term based on usage, save that any outstanding payments during a Subsequent Term as at 31 March 2023 or 31 March 2024 respectively shall be immediately invoiced to the Customer in accordance with agreed estimated usage;</p> <p>9.5.5 apply any payments made by the Customer during a Subsequent Term which exceed the Charges to any Subsequent Term or, if no Subsequent Term is entered into, refund those payments to the Customer within thirty (30) days of the expiry of the relevant Subsequent Term;</p> <p>9.5.6 be entitled to payment of any Charges in excess of payments made by the Customer under clause 9.5.4 above within thirty (30) days of supplying the Customer with a compliant invoice following the expiry of the relevant Subsequent Term; and,</p> <p>9.5.7 the Supplier shall, upon commencement of the Initial</p>

				Term of the Agreement only. be entitled to s43(2) In respect of development fees within thirty (30) days of supplying the Customer with a compliant Invoice; 9.5.8 Ensure that all invoices and payment communications must quote the Purchase Order number stated on the Order Form.
5.	Amends existing clause	Part A	Clause 9.9	Payment by the Customer shall be without prejudice to any claims or rights the Customer and any other Service Recipient may have against the Service Provider and shall not constitute an admission by the Customer as to the performance of the Service Provider's obligations under this Agreement.
6.	Amends existing clause	Part A	Clause 10.2	The Service Provider warrants and undertakes to the Customer and, in respect of clauses 10.2.5, 10.2.6, 10.2.10 and 10.2.11 also to the Service Recipients, that:
7.	Amends existing clause	Part A	10.2.5	It is authorised to use the Third-Party Software and any third-party systems in connection with its obligations under this Agreement and shall remain so authorised for the duration of this Agreement and shall be authorised by the relevant licensors and owners to grant the rights for the Customer's and Service Recipients' use;
8.	Amends existing clause	Part A	10.2.6.1	any executable code in the Live system which has not passed the Acceptance Tests by the Customer or Service Recipient; or
9.	Amends existing clause	Part A	10.2.7.2	the Support Materials shall provide adequate instructions to enable the Customer and other Service Recipients to make proper use of the facilities and functions; and
10.	Amends existing clause	Part A	10.3	If the Service Provider receives written notice from the Customer or another Service Recipient at any time after any Go-Live Date of any breach of the warranties herein stipulated (in so far as applicable to the Customer or relevant Service Recipient), the Service Provider shall immediately after receiving such notice take steps to remedy the defect or error in question and shall use best endeavours to promptly resolve the defect or error in question.
11.	Amends existing clause	Part A	11.2.2	ensure continuing integration with the Customer's and other Service Recipients' existing systems as identified by the Customer, and seamlessly interfaces to the Customer's and third-party systems as specified in the Deliverables (Part F, 1, of Tender Documents);
12.	Amends existing clause	Part A	11.2.3	co-operate with the Customer's Representative, officers, employees and other independent consultants, and those of other Service Recipients, whenever necessary or desirable in the performance of IT Services;
13.	Amends existing clause	Part A	11.2.11	ensure that the Service Provider's personnel comply with the Customer's requirements for the conduct of staff when on the Customer's premises, and with the relevant Service Recipients' requirements when on their premises, respectively.
14.	Amends existing clause	Part A	11.4	Where the Service Provider has purchased Third Party Software, the Service Provider shall pay for the Third-Party Software within the time allowed by the third party and shall not put at risk the Customer's and other Service Recipients' possession and use of the Third-Party Software after delivery to the Customer.

15.	Amends existing clause	Part A	11.7	The Service Provider shall, as a continuing obligation throughout the term of this Agreement, where Software is used in the provision of IT Services or information uploaded, interfaced or exchanged with the Customer's or other Service Recipients' systems, use the most up-to-date antivirus from an industry- accepted antivirus software vendor. The Service Provider shall check for, contain the spread of, and minimise the impact of malicious software.
16.	Amends existing clause	Part A	11.8	If malicious software is found, the Service Provider shall co-operate with the Customer and any other affected Service Recipient to reduce the effect of the malicious software. If malicious software causes loss of operational efficiency or loss or corruption of the Customer Data, the Service Provider shall use its best endeavours to help the Customer and any other affected Service Recipient to mitigate any losses and restore the provision of IT Services to the desired operating efficiency as soon as possible.
17.	Amends existing clause	Part A	12.2	The Customer agrees to provide guidance to the Service Provider on the Customer's business practices and those of other Service Recipients which affect IT Services.
18.	Amends existing clause	Part A	12.5	If requested by the Service Provider and agreed by the Customer to be necessary and expedient to the Service Provider's compliance with its obligations under this Agreement, the Customer shall provide a desk and wi-fi facilities for the use of the Service Provider on a licence-at-will basis.
19.	Amends existing clause	Part A	13.2.2	13.2.2 If the Service Provider fails to: 13.2.2.1 deliver a Deliverable by its associated delivery date and fails to remedy the failure within 7 days or such longer timescale as may be specified by the Customer in writing; 13.2.2.2 comply with a Correction Plan and fails to remedy the failure within 7 days or such longer timescale as may be specified by the Customer in writing; 13.2.2.3 meet a Service Level target on a repeated and/or persistent basis; or 13.2.2.4 pass the repeat Acceptance Tests and fails to remedy the failure within 7 days or such longer timescale as may be specified by the Customer in writing;
20.	Amends existing clause	Part A	13.7	Any termination of this Agreement (howsoever occasioned) shall not affect any accrued rights or liabilities of either Party or any Service Recipient.
21.	Amends existing clause	Part A	14.1	Following the service of a termination notice by the Customer or the Service Provider for any reason under this clause 13, the Service Provider shall continue to be under an obligation to provide IT Services to the required Service Levels and to ensure that there is no degradation in the standards of IT Services until the date of termination.
22.	Amends existing clause	Part A	14.2.2.1	the Customer's and other Service Recipients' Confidential Information under its control or in its possession;
23.	Amends existing clause	Part A	14.2.2.2	the Customer Data, or media containing the Customer Data or other materials provided by the Customer or other Service Recipients; and
24.	Amends existing clause	Part A	14.2.2.3	the Customer or other Service Recipient owned property in the possession or control of the Service Provider or its sub-contractors, to the Customer or relevant Service Recipient;

25.	Inserts additional clause	Part A	14.3	For the avoidance of doubt, the termination by a Service Recipient of a Contract entered into with the Service Provider in accordance with Part A, clause 5.5 (as Inserted by Part J, special term 2) and Part K, shall not have the effect of automatically terminating or otherwise reducing the Term of this Agreement.
26.	Amends existing clause	Part A	15.1	Notwithstanding any other provision in this Agreement, the Service Provider neither excludes nor limits liability to the Customer (or, where explicitly provided for in this Agreement, to any Service Recipient) for any claims, losses (including regulatory losses and fines), damages, costs or expenses, or acts or omissions arising from:
27.	Amends existing clause	Part A	15.2	Except as provided in clause 15.1 above, the Service Provider's total liability to the Customer and any other Service Recipient for any claims, losses, damages, costs and expenses arising under this Agreement or otherwise for any cause whatsoever shall be limited to the sum of the relevant insurance cover in clause 16 below.
28.	Amends existing clause	Part A	15.4	Except as otherwise prohibited by law, the total liability of the Customer and any other Service Recipient to the Service Provider for any claims, losses, damages, costs and expenses arising under this Agreement or otherwise for any cause whatsoever, shall be limited to the value of the monies paid to the Service Provider under this Agreement.
29.	Amends existing clause	Part A	15.5	In no event shall the Customer and/or Service Recipients or any of them of the one part, or the Service Provider of the other, be liable to the other for any loss of profits, business, revenue, damage to goodwill, savings or any indirect, special or consequential loss or damage.
30.	Amends existing clause	Part A	17.5	The Intellectual Property Rights of the Service Provider's Software and any modifications created outside of this Agreement and the Agreement between The Police and Crime Commissioner for Derbyshire and Pervade Software Limited for the Provision of a Network Traffic Analyser, which was novated to the Customer effective from 01 April 2021, is the Background IPR of the Service Provider and/or its licensors.
31.	Amends existing clause	Part A	17.6	All Bespoke Work created by the Service Provider for and under this Agreement and the Agreement between The Police and Crime Commissioner for Derbyshire and Pervade Software Limited for the Provision of a Network Traffic Analyser, which was novated to the Customer effective from 01 April 2021, vests in the Customer and is the Customer's Foreground IPR. Without limitation, Bespoke Work shall include any code, rules, machine learning models, algorithms, documentation, branding, website design and content etc. The Service Provider grants to the Customer a perpetual, non-revocable, transferable and sublicensable worldwide licence in any of the Service Provider's Background IPR embedded in the Bespoke Work.
32.	Amends existing clause	Part A	17.10	All Intellectual Property Rights in the Customer's software and Customer Data created for and under this Agreement is the Customer's and/or its licensors' Foreground IPR.
33.	Amends existing clause	Part A	17.11	The Service Provider shall have no rights to use the Customer's names, logos or trademarks or those of the other Service Recipients without the Customer's prior written approval.
34.	Amends	Part A	17.12	The Customer grants to the Service Provider a limited, non-

	existing clause			transferable, non-exclusive, royalty- free licence to use only such of the Customer's and its licensors' Intellectual Property Rights as is required, solely to enable the Service Provider to deliver the IT System and to perform the Services.
35.	Amends existing clause	Part A	17.13	17.13 The Service Provider shall procure that all moral rights of its authors (including that of its sub- contractor's authors) arising from the performance of this Agreement are waived. The Service Provider shall indemnify the Customer and other Service Recipients in the event of any claims, actions or proceedings for any costs, losses, damages, or expenses brought by the author against the Customer or any other Service Recipient.
36.	Amends existing clause	Part A	18.1	The Service Provider shall defend at its own expense any claim brought against the Customer or other Service Recipient alleging that the use of the IT System infringes the Intellectual Property Rights of a third party ('Intellectual Property Claim') and the Service Provider shall pay all costs and damages awarded or agreed to in settlement of an Intellectual Property Claim provided that the Customer or Service Recipient:
37.	Amends existing clause	Part A	18.2.1	obtain for the Customer and other Service Recipients the right to continue using the IT System which is the subject of the Intellectual Property Claim; or
38.	Amends existing clause	Part A	18.3	If the remedies set out in clause 18.2 above are not in the Service Provider's opinion reasonably available, the Customer and the other Service Recipients shall cease using the IT System which is the subject of the Intellectual Property Claim, the Service Provider shall repay to the Customer all sums paid to the Service Provider and indemnify the Customer for all damages, losses, costs and expenses including reasonable legal expenses and third party claims suffered by the Customer.
39.	Amends existing clause	Part A	18.4	Any replacement or modification made to the IT System under clause 18.2.2 shall be subject to the same warranties and terms of this Agreement and the Customer and other Service Recipients shall have the same rights as if they were made on the Commencement Date.
40.	Amends existing clause	Part A	18.6	If the Service Provider learns of any claim of infringement of the Customer's or other Service Recipients' Intellectual Property Rights in the Customer Data, it shall promptly notify the Customer and the respective Service Recipient. The Service Provider shall do all such things as the Customer or relevant Service Recipient may reasonably require at the Customer's or relevant Service Recipient's expense to assist the Customer or relevant Service Recipient in taking proceedings or any other actions the Customer or relevant Service Recipient may reasonably take to terminate or prevent any such claim.
41.	Amends existing clause	Part A	19.1	Both parties to this Agreement undertake, except as provided below, to treat as confidential and keep secret all information marked 'confidential' or which may reasonably be supposed to be confidential, including, without limitation, information contained or embodied in the Deliverables in Part F, 1 of the Tender Documents and other information supplied by the Customer, other Service Recipient or Service Provider (in this Agreement collectively referred to as 'Confidential Information') with the same degree of care as it employs with

				regard to its own confidential information of a like nature and in any event in accordance with best current commercial security practices, provided that, this clause shall not extend to any Information which was rightfully in the possession of either party prior to the commencement of the negotiations leading to this Agreement or which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause).
42.	Amends existing clause	Part A	19.2	A party shall not without the prior written consent of the other party divulge any part of the Confidential Information to any person, other than a Service Recipient as necessary, except:
43.	Amends existing clause	Part A	19.2.4	to any person who is for the time being appointed by either party or a Service Recipient to maintain the equipment on which the Software is for the time being used (in accordance with the terms of the Agreement) and then only to the extent necessary to enable such person to properly maintain the equipment.
44.	Insert additional clause	Part A	19.2.5	To any person who is for the time being appointed by the Customer or the Customer's Representative to carry out functions related to the maintenance of public confidence in the legal, regulatory and ethical compliance of Police CyberAlarm.
45.	Amends existing clause	Part A	19.3	Both parties undertake to ensure that persons and bodies referred to in clause 19.2 are made aware before the disclosure of any part of the Confidential Information that the same is confidential and that they owe a duty of confidence to the other party and to other Service Recipients.
46.	Amends existing clause	Part A	19.4	Each party to this Agreement shall promptly notify the other party, or the relevant Service Recipient in addition to the Customer if applicable, if it becomes aware of any breach of confidence by any person to whom it divulges all or any part of the Confidential Information and shall give the other party, and the relevant Service Recipient if applicable, all reasonable assistance in connection with any proceedings which the other party or the relevant Service Recipient may institute against such person for breach of confidence.
47.	Amends existing clause	Part A	20.1	The Customer and/or the relevant Service Recipients shall own (or shall have the right to use) all right, title and interest in and to the Customer Data.
48.	Amends existing clause	Part A	21.1	The Service Provider acknowledges that the Customer and other Service Recipients are subject to the requirements of the Code of Practice on Access to Government Information, the Freedom of Information Act 2000 ("FOIA") and the Environmental Information Regulations 2004 ("EIR"), in addition to common law obligations in relation to the right of access to public information.
49.	Amends existing clause	Part A	21.2	The Service Provider shall assist and co-operate with the Customer and any other Service Recipient in a timely and efficient manner and provide a copy of all information in its possession or power, in the form that the Customer or relevant Service Recipient requires, to enable the Customer or other Service Recipient to respond to a request for information within the time for compliance set out in Section 10 of the FOIA.
50.	Amends	Part A	21.4	Part F, 2c shall list the class or category of information or the

	existing clause			information itself and shall specify which exemptions under the FoIA apply to each specified class category or specific information. Each case shall indicate when it is likely that the information can be made available under the FoIA or if the information is unlikely ever to be made so available that this is the case. Where such information is exempt under the rules governing commercial matters (s.43(2) FoIA) then unless special circumstances apply it shall not be withheld under the FoIA for more than seven (7) years after the expiry or termination of this Agreement. The Customer shall notify such classes or categories of information to the other Service Recipients.
51.	Amends existing clause	Part A	21.5	Information relating to the overall value performance or completion of this Agreement, or relating to contract records and administration, shall not be accepted as reserved information. The Customer or other Service Recipient may however withhold access to such information under the FoIA or other applicable law in appropriate cases.
52.	Amends existing clause	Part A	21.6	The Service Provider acknowledges that the Customer or other Service Recipient may, acting in accordance with the Department of Constitutional Affairs' Code of Practice on the Discharge of Functions of Public Authorities under Part I of the Freedom of Information 2000, be obliged under the Code of Practice on Access to Government Information, the FOIA, or the Environmental Information Regulations or common law obligations in relation to the right of access to public information to disclose information without consulting with the Service Provider, or following consultation with the Supplier and having taken its views into account.
53.	Amends existing clause	Part A	21.7	Should it subsequently transpire that any information has been incorrectly classified as reserved information by the Service Provider or any competent public authority orders the information to be released, the Service Provider shall immediately deliver such information to the Customer or other relevant Service Recipient and reimburse all the costs incurred by the Customer or other relevant Service Recipient as a result of the Service Provider seeking to classify the information as reserved information.
54.	Amends existing clause	Part A	21.8	The Service Provider shall ensure that all information produced in the course of the Agreement or relating to this Agreement is retained for disclosure and shall permit the Customer or other relevant Service Recipient to inspect such records as requested from time to time. The Service Provider acknowledges that any lists or schedules provided by it outlining Confidential Information are of indicative value only and that the Customer or other relevant Service Recipient may nevertheless be obliged to disclose Confidential Information in accordance with clause 19.2.3.
55.	Amends existing clause	Part A	22.1	The Customer or other Service Recipient may, during the continuance of this Agreement refuse admission to their respective premises of any of the Service Provider's personnel whom the Customer or other Service Recipient believe represents a security risk, and the Customer may require the Service Provider to exclude such personnel from working on the IT Services or IT Services under this Agreement or if the Customer believes the personnel do not have the required

				levels of training and expertise or where the Customer has other grounds for doing so. The decision of the Customer or other Service Recipient shall be final, and It shall not be obliged to provide any reasons.
56.	Amends existing clause	Part A	22.2.1	use Its best endeavours to keep confidential the passwords or other security Information relating to the IT Services or any equipment of the Customer or other Service Recipient;
57.	Amends existing clause	Part A	22.2.3	regularly review Its security policies and the actual security of the IT Services, and inform the Customer of any additional measures necessary to maximise security of the IT Services and integrity of the Customer Data, and other Customer and Service Recipient information;
58.	Amends existing clause	Part A	22.2.4	notify the Customer, followed by any other relevant Service Recipient, promptly of any unauthorised access or use of the Customer Data or other security incident affecting Its network and information systems that could potentially affect the Customer or other Service Recipient, and respond without delay to all queries and requests for information from the Customer or other Service Recipient, whether discovered by the Service Provider or the Customer or other Service Recipient, in particular bearing in mind the extent of the Customer's and other Service Recipients' reporting obligations under applicable network and information security legislation and that the Customer may be required to comply with statutory or other regulatory timescales;
59.	Amends existing clause	Part A	22.2.12	co-operate with the Customer and other Service Recipients in all aspects of Its compliance with the Network and Information Systems Regulations including, without limitation, any requests for information in the event of a suspected or actual security incident and any inspections by regulators.
60.	Amends existing clause	Part A	22.4	The Service Provider shall comply with the Customer's or relevant Service Recipient's Health & Safety policies and procedures while on the Customer's or Service Recipients' premises.
61.	Amends existing clause	Part A	23.1	The Service Provider shall In the performance of the IT Services take account of any statute, statutory Instrument, byelaw, relevant British Standard (or equivalent EU standard) or other mandatory requirement or code of practice and the Customer's policies or other Customer requirements notified to the Service Provider, which may be in force, or come into force, during the performance of the IT Services.
62.	Inserts new clause	Part A	25.2	For the avoidance of doubt, clause 25.1 above shall not restrict the parties and any Service Recipient from entering into a partnership, joint venture or other relationship, including in connection with rights granted under this Agreement, as envisaged in the Specification.
63.	Amends existing clause	Part A	35.3	Sub-contracting the IT Services shall not entitle the Service Provider to charge an administration fee nor require the Customer or other Service Recipient to enter into an agreement with the third-party. All requisite third- party licences shall be held by the Service Provider for the benefit of the Customer.
64.	Amends existing clause	Part A	35.4	The Service Provider shall indemnify the Customer, and any relevant Service Recipient in so far as the Service Recipient would have been entitled to such indemnity under the terms

				of this Agreement had the loss or damage arisen from any act or omission of the Service Provider, against any loss or damage suffered by the Customer or other Service Recipient arising from any act or omission of such agents or sub-contractors.
65.	Amends existing clause	Part A	37.1	Each party shall bear its own legal costs and other costs and expenses arising in connection with the drafting, negotiation, execution and registration (if applicable) of this Agreement, and any other agreements the parties are required to enter into as specified in this Agreement.
66.	Amends existing clause	Part A	39.1	Save as expressly set out in this Agreement in relation to Service Recipients, a person who is not a Party to the Agreement shall have no right to enforce any of its provisions which, expressly or by implication, confer a benefit on him, without the prior written agreement of the Parties. This clause 30.1 does not affect any right or remedy of any person which exists or is available apart from the Contracts (Rights of Third Parties) Act 1999.
67.	Insert additional clause	Part A	39.2	No consent of a Service Recipient is necessary for any variation or termination of the Agreement or any one or more clauses of it.
68.	Insert additional clause	Part A	39.3	In so far as relates to the Customer, no consent of a Service Recipient is necessary for any release or compromise in whole or in part of any liability.
69.	Amends existing clause	Part A	43.1	If any dispute arises between the parties in connection with this Agreement, a director or other senior representative of the parties with authority to settle the dispute shall, within 14 days of a written request from one party to the other, meet in good faith to resolve the dispute.
70.	Amends existing clause	Part B	1	This SLA describes the minimum level of support and maintenance services to be provided by the Service Provider to the Customer and other Service Recipients and the respective obligations of the parties.
71.	Amends existing clause	Part B	2.1	'Permitted Purpose' in the case of reverse analysis where permitted by applicable law, the Customer or other Service Recipient may decompile the Software if it is essential to do so in order to achieve interoperability of the IT System with another software program or media;
72.	Amends existing clause	Part B	2.1	'Support Request' A request made by the Customer or other Service Recipient for support of the Software or IT System, including the correction of a Fault;
73.	Amends existing clause	Part B	3.4	The Service Provider shall give the Customer and other Service Recipients notice in accordance with the specification of any planned maintenance work which shall affect the availability of the IT System and shall plan and carry out such work at such times so as to minimise disruption to the availability of the IT System.
74.	Amends existing clause	Part B	3.7	The Support Services to be provided to the Customer and other Service Recipients shall include:
75.	Amends existing clause	Part B	3.8	The Customer and other Service Recipients may request Support Services by way of a Support Request. The Support Request shall contain a detailed description of the problem or Fault and where known the start time of the incident. The Customer or other Service Recipient shall telephone or document to the Service Provider a detailed description of any

				Fault requiring Support Services and the circumstances in which it arose, forthwith upon becoming aware of the same, so that it can be replicated. The Customer or other Service Recipient shall provide such additional information as may be reasonably requested by the Service Provider to enable the Fault to be classified in accordance with paragraph 3.13 below.
76.	Amends existing clause	Part B	3.13	'Critical Fault' means any fault which is fatal, or disables major functions of the Customer's or Service Recipient's business or marketability of its services or products which results in the IT System, Software or media being non-operational for business-critical delivery;
77.	Amends existing clause	Part B	3.13	'Important Fault' means a Fault which has degraded operations or errors disabling only certain non-essential functions and which is agreed to be important by the Service Provider and the Customer or Service Recipient but does not constitute a Critical Fault or a Major Fault;
78.	Amends existing clause	Part B	3.13	'Minor Fault' means a Fault which has minimal impact and is agreed to be minor by the Service Provider and the Customer or Service Recipient, but which does not constitute a Critical Fault, Major Fault or Important Fault (for example errors in documentation and spelling errors in non-public facing forms/screens);
79.	Amends existing clause	Part B	3.14	If the parties agree a Fault classification, the Service Provider shall use all reasonable endeavours within the Resolution Times of such agreement (or sooner if reasonably practicable) to fix the Fault and/or supply instructions to the Customer and other Service Recipients, which are intended to provide a work around acceptable to the Customer for the Fault or provide a correction.
80.	Amends existing clause	Part B	3.15	If the parties, acting with due diligence, are unable to agree on the designation of a Fault reported by the Customer or other Service Recipient pursuant to paragraph 3.4 above, the Service Provider shall, acting reasonably, designate the level of Fault and references to "agree" and "agreement" in paragraph 3.14 above shall be deemed to refer to the designation of the Fault by the Service Provider; and
81.	Amends existing clause	Part B	3.17	In order for the Service Provider to be able to provide the Support Services to the Customer and other Service Recipients, the Customer shall:
82.	Amends existing clause	Part B	3.19	The Service Provider shall give the Customer and any affected Service Recipient regular updates of the nature and status of its efforts to correct any Fault and shall give the Customer monthly reports as to achievement of Service Levels and Service Credits to which the Customer has become entitled.
83.	Amends existing clause	Part B	3.20	The Service Provider shall in respect of Critical and Major Faults report to the Customer and any other affected Service Recipient and the Service Provider shall provide an update of work being undertaken to circumvent or provide a correction to the Fault at least once a day, the first such update to be provided within one (1) Hour of the designation of the Fault as a Critical Fault, or such other frequency as shall be agreed between the parties from time to time.
84.	Amends existing clause	Part B	4.3	The Service Provider shall make all commercially reasonable efforts to provide the Customer and other Service Recipients with prior email notification of all scheduled and emergency

				Outages in accordance with the Specification.
85.	Amends existing clause	Part B	11.1	"Downtime" means the total time during the Support Hours in the calendar month during which the service is not available excluding (i) permitted downtime during the same hours and (ii) time during the same hours during which the service is not available due to a Fault which lies with the Customer or other Service Recipient. ("X")
86.	Amends existing clause	Part B	11.2	"Downtime" means the total time outside the Support Hours in the calendar month during which the service is not available excluding (i) permitted downtime during the same hours and (ii) time during the same hours during which the service is not available due to a Fault which lies with the Customer or other Service Recipient. ("X")
87.	Amends existing clause	Part B	13.1	Releases shall be applied to the TEST and TRAIN systems and the Customer and other Service Recipients informed of the changes and be given a reasonable time in the circumstances to test and where necessary retrain staff before the Release is applied to the LIVE system.
88.	Amends existing clause	Part B	13.3	The Service Provider shall notify the Customer and other Service Recipients in advance of any Releases that require Downtime or service interruption, and such Releases will be applied to the LIVE system at times agreed by the Service Provider and the Customer. In the event that such advance notice coincides with significant activity periods of the Customer then the parties will agree an alternative time for applying the Release (acting reasonably).
89.	Amends existing clause	Part C		'Background IPR' the Intellectual Property Rights of a party or other Service Recipient which existed prior to the date of the Agreement, or which has been created outside the scope or contemplation of the Agreement;
90.	Amends existing clause	Part C		'Bespoke Work' Work which is created solely and exclusively at the time of creation for the Customer.
91.	Amends existing clause	Part C		'Customer Cause' where a Delay to a Milestone is caused either wholly or partly by the Customer's or other Service Recipient's actions or omissions;
92.	Amends existing clause	Part C		'Customer Data' the data, information, text, media content, features, products, services, advertisements, promotions, ontology, Links, pointers, technology, software and databases for publication (including without limitation, literary, artistic, audio and visual content), including any publication or information created by or for the Customer or other Service Recipient, for the IT Services;
93.	Amends existing clause	Part C		'Support Materials' the operating manuals (including electronic), user instructions, technical literature and documentation provided to the Customer and other Service Recipients to facilitate the support of the IT Services;
94.	Inserts additional clause	Part C		'Service Recipient' any police force identified in Police Act 1996 Schedule 1, in addition to the Metropolitan Police Service, the City of London Police, Police Scotland, the Police Service of Northern Ireland, North Wales Police, South Wales Police, Dyfed-Powys Police and Gwent Police.
95.	Inserts additional clause	Part D		For the purposes of this Part D, unless specified below, terms shall bear the same meaning as in the Agreement
96.	Amends	Part D		Agreement: means the Agreement for the provision of the

	existing clause			next iteration of the Police CyberAlarm, including additional functionality in respect of ingesting / enriching / categorising firewalls, analysis and event reporting, and scanning of external IP / websites of member organisations, to provide enriched intelligence source for policing and other developments between The Mayor and Commonalty and Citizens of the City of London and Pervade Software Ltd entered into on 01 November 2021;
97.	Deletes existing clause	Part D		Customer: means the Data Service Provider;
98.	Amends existing clause	Part D		Data Protection Impact Assessment: an assessment by the Customer for and on behalf of any Controller of the impact of the envisaged processing on the protection of Personal Data;
99.	Amends existing clause	Part D	1.1	The Parties acknowledge that for the purposes of the Data Protection Legislation, Customer and/or the other Service Recipients are the respective Controllers, and the Service Provider is the Processor. The only processing that the Service Provider is authorised to do is listed in Annex 1 by Customer for and on behalf of the Controllers and may not be determined by the Service Provider.
100.	Amends existing clause	Part D	1.2	The Service Provider shall notify Customer immediately if it considers that any of Customer's instructions, or those of any Controller, infringe the Data Protection Legislation.
101.	Amends existing clause	Part D	1.4(a)	process that Personal Data only in accordance with Annex 1, unless the Service Provider is required to do otherwise by law. If it is so required, the Service Provider shall promptly notify Customer and any relevant Controller before processing the Personal Data unless prohibited by law;
102.	Amends existing clause	Part D	1.4(b)	ensure that it has in place Protective Measures, which have been reviewed and approved by Customer for and on behalf of the Controllers as appropriate to protect against a Data Loss Event having taken account of the:
103.	Amends existing clause	Part D	1.4(c)(ii)(C)	are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by Customer and/or relevant Controller (in respect of Personal Data of which it is the relevant Controller) or as otherwise permitted by this Agreement; and
104.	Amends existing clause	Part D	1.4(d)	not transfer Personal Data outside of the EU unless the prior written consent of Customer for and on behalf of the Controllers has been obtained and the following conditions are fulfilled:
105.	Amends existing clause	Part D	1.4(d)(iv)	the Service Provider complies with any reasonable instructions notified to it in advance by Customer for and on behalf of the Controllers with respect to the processing of the Personal Data;
106.	Amends existing clause	Part D	1.4(e)	at the written direction of Customer, delete or return Personal Data (and any copies of it) to Customer and/or relevant Controller (in respect of Personal Data of which it is the relevant Controller) on termination of the Agreement unless the Service Provider is required by law to retain the Personal Data.
107.	Amends existing clause	Part D	1.5	Subject to clause 1.6, the Service Provider shall notify Customer and/or relevant Controller (in respect of Personal Data of which it is the relevant Controller) promptly and

				without any undue delay if it:
108.	Amends existing clause	Part D	1.6	The Service Provider's obligation to notify under clause 1.5 shall include the provision of further information to Customer and/or the relevant Controller (in respect of Personal Data of which it is the relevant Controller) in phases, as details become available.
109.	Amends existing clause	Part D	1.7	Taking into account the nature of the processing, the Service Provider shall provide Customer and/or the relevant Controller (in respect of Personal Data of which it is the relevant Controller) with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by Customer and/or relevant Controller (in respect of Personal Data of which it is the relevant Controller)) including by promptly providing:
110.	Amends existing clause	Part D	1.7(a)	Customer and/or relevant Controller (in respect of Personal Data of which it is the relevant Controller) with full details and copies of the complaint, communication or request;
111.	Amends existing clause	Part D	1.7(b)	such assistance as is reasonably requested by Customer and/or relevant Controller (in respect of Personal Data of which it is the relevant Controller) to enable it to comply with a Data Subject Access Request, or request to rectify, block or erase Personal Data, within the relevant timescales set out in the Data Protection Legislation;
112.	Amends existing clause	Part D	1.7(c)	Customer and/or relevant Controller (in respect of Personal Data of which it is the relevant Controller), at its request, with any Personal Data it holds in relation to a Data Subject;
113.	Amends existing clause	Part D	1.7(d)	assistance as requested by Customer and/or relevant Controller (in respect of Personal Data of which it is the relevant Controller) following any Data Loss Event;
114.	Amends existing clause	Part D	1.7(e)	assistance as requested by Customer and/or relevant Controller (in respect of Personal Data of which it is the relevant Controller) with respect to any request from the Information Commissioner's Office, or any consultation by Customer and/or relevant Controller (in respect of Personal Data of which it is the relevant Controller) with the Information Commissioner's Office.
115.	Amends existing clause	Part D	1.8	The Service Provider shall maintain complete and accurate records and information to demonstrate its compliance with this Part D.
116.	Deletes existing clause	Part D	1.8(a)-(c)	
117.	Amends existing clause	Part D	1.9	The Service Provider shall allow for and contribute to audits of its Data Processing activity by Customer or Customer's designated auditor for and on behalf of the Controllers which, unless in response to any failure to comply with the terms of this Part or notification of a Personal Data Breach or at the direction of an applicable supervisory authority, shall take place no more than once in any 12 month period and shall be on at least 7 days' notice to the Service Provider. In the event of any failure to comply with the terms of this Part or notification of a Personal Data Breach or at the direction of an applicable supervisory authority, the Customer shall be entitled to carry out such additional audits as it deems

				appropriate in the subsequent 12 month period.
118.	Amends existing clause	Part D	1.11(b)	obtain the written consent of Customer for and on behalf of the Controllers;
119.	Amends existing clause	Part D	1.12	The Service Provider shall remain fully liable to the Customer and the Controllers for all acts or omissions of any Sub-processor.
120.	Amends existing clause	Part D	1.13	The Customer may, at any time on not less than 30 Working Days' notice, revise this Part D by replacing, amending or supplementing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).
121.	Amends existing clause	Part D	1.14	1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Customer may on not less than 30 Working Days' notice to the Service Provider amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.
122.	Amends existing clause	Part D	1.15	Notwithstanding any other provision in the Agreement, the Service Provider shall indemnify the Customer and/or relevant Controller (in respect of Personal Data of which it is the relevant Controller) in respect of any, fine, loss, claim, action, damages or demand imposed on or suffered as a result of any breach by the Service Provider of this Part D.
123.	Amends existing clause	Part H		<p>We, Pervade Software Ltd, certify that ALL of the following:</p> <ol style="list-style-type: none"> the Customer's and Service Recipients' Confidential Information under its control or in its possession. the Customer Data, or media containing the Customer Data or other materials provided by the Customer and/or any Service Recipient; and the Customer and/or Service Recipient owned property in the possession or control of the Service Provider, to the Customer or relevant Service Recipient; <p>have been returned, destroyed or deleted in accordance with the Agreement dated [date].</p> <p>Signed by Board Director [SERVICE PROVIDER] Date</p>
124.	Inserts additional part	Part K		

PART K
TEMPLATE CONTRACT BETWEEN THE SERVICE PROVIDER AND THE SERVICE RECIPIENT

This Contract is made between:

- 1) **[INSERT TITLE OF CHIEF CONSTABLE/COMMISSIONER]** of **[INSERT REGISTERED ADDRESS]**
(a "Service Recipient"); and,
- 2) Pervade Software Ltd of Castle Court, 6 Cathedral Road, Cardiff, CF11 9LJ (the "Service Provider")
(together, 'the Parties').

WHEREAS The Mayor and Commonalty and Citizens of the City of London of Guildhall, PO BOX 270, London EC2P 2EJ have entered into an Agreement with Pervade Software Ltd of Castle Court, Cardiff, CF11 9LJ dated **[INSERT DATE]** for the provision of Police CyberAlarm

AND WHEREAS that Agreement grants the Customer the right to licence Police CyberAlarm and its constituent parts to other law enforcement entities, defined in that agreement as 'Service Recipients'

AND WHEREAS the Service Recipients are granted certain rights and benefits under that Agreement

AND WHEREAS the Service Provider requires, as a condition of the grant of licences to the Service Recipients, that the Service Recipients provide certain warranties and indemnities to the Service Provider

AND WHEREAS the Service Recipients and Service Provider wish to comply with their respective obligations under the Data Protection Legislation and other Law

1. Definitions

1.1. Unless otherwise detailed below, words and phrases used in this Contract shall have the same meaning as in the Agreement, unless the context otherwise requires:

- 1.1.1. **'Agreement'** means the agreement for the IT Services described in the Order Form **[INSERT PURCHASE ORDER NUMBER]** issued by the Customer comprising the Particulars, the Standard Terms and Conditions and the Special Terms and Conditions, if any.
- 1.1.2. **'Background IPR'** means the Intellectual Property Rights of a Party which existed prior to the date of the Contract and Agreement, or which have been created outside the scope or contemplation of the Contract and Agreement.
- 1.1.3. **'Commencement Date'** means the date of commencement of the Agreement, being 31 October 2021.
- 1.1.4. **'Service Recipient Data'** means the Data, information, text, media content, features, products, services, advertisements, promotions, ontology, Links, pointers, technology, software, and databases for publication (including without limitation, literary, artistic, audio and visual content), including any publication or information created by or for the Service Recipient in the context of the IT Services, and shall include Content and CRM Information, which shall form part of the Customer Data.
- 1.1.5. In this Contract, the expressions **'Data'**, **'Controller'**, **'Data Subject'**, **'Processor'**, **'Processing'**, **'Personal Data'**, and **'Personal Data Breach'** have the same meaning as in Article 4 of GDPR.
- 1.1.6. **'Data Protection Legislation'** means (i) The General Data Protection Regulation (Regulation (EU) 2016/679), the Law Enforcement Directive (EU) 2016/680), the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003), the Protection of Freedoms Act 2012, and any applicable implementing laws as amended from time to time; (ii) the Data Protection Act 2018; and (iii) all applicable law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Service Provider is bound to comply about the processing of personal data and privacy.

- 1.1.7. **'Foreground IPR'** means the Intellectual Property Rights created pursuant to and in contemplation of the Agreement as part of the project.
- 1.1.8. **'Initial Term'** means the period expiring one year from the Commencement Date.
- 1.1.9. **'Subsequent Term'** means the two (2) one (1) year periods commencing on an anniversary of the Commencement Date following expiry of the Initial Term or a previous Subsequent Term.
- 1.1.10. **'Sub-processor'** means any third party appointed to process Personal Data on behalf of the Service Provider related to the Agreement and this Contract.
- 1.1.11. **'Intellectual Property Rights'** or **'IPR'** means any copyright, database rights, design rights, domain name rights, patents, trademarks or service marks and all other intellectual property rights whether registered or not, and applications for such rights.
- 1.1.12. **Criminal Conviction and Offence Data** has the same meaning as in s11(2) Data Protection Act 2018.
- 1.1.13. **GDPR** means the General Data Protection Regulation (Regulation (EU) 2016/679).
- 1.1.14. **LED** means the Law Enforcement Directive (Directive (EU) 2016/680).
- 1.1.15. **Data Loss Event** means any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach.
- 1.1.16. **Police Data** means any Data including Personal Data and Special Categories of Personal Data, to be provided to, or collected by, the Processor and processed on behalf of the Controller as identified in this Contract.
- 1.1.17. **Contract** means this Data Processing Contract together with its schedules and all other documents attached to or referred to as forming part of this Contract.
- 1.1.18. **Law** means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, byelaw, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply.
- 1.1.19. **Lead Controller** shall mean the Commissioner of the City of London Police, or such other Service Recipient or other entity as may be notified to the Service Provider in writing from time to time.
- 1.1.20. **Access to Information Legislation** means the Freedom of Information Act 2000 ("FoIA"), the Environmental Information Regulations 2004 ("EIR"), the Code of Practice on Access to Government Information, and any common law obligations in relation to the right of access to public information.

2. Interpretation

- 2.1. Headings are inserted for convenience only and shall not affect the construction or interpretation of this Contract and, unless otherwise stated, references to clauses and schedules are references to the clauses of and schedules to this Contract;
- 2.2. Any reference to any enactment or statutory provision shall be deemed to include a reference to such enactment or statute as extended, re-enacted, consolidated, implemented or amended and to any subordinate legislation made under it.
- 2.3. The word 'including' shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and the word 'include' and its derivatives shall be construed accordingly.
- 2.4. In the event of any conflict between, on the one hand, the terms of the Agreement and, on the other hand, the terms of this Contract, the terms of the Agreement shall prevail.

3. Entire Agreement

- 3.1. Without prejudice to the rights and obligations granted to and/or imposed upon the Parties under the Agreement, except for fraud and fraudulent misrepresentation, this Contract supersedes all prior agreements, arrangements and undertakings between the Parties and constitutes the entire agreement between the parties relating to the subject matter of this Contract. The parties confirm that they have not entered into this Contract on the basis of any representation that is not expressly incorporated herein.

4. Duration

- 4.1. This Contract shall start on the later of:

- 4.1.1. the Commencement Date; or,
- 4.1.2. the date it is signed by the Service Recipient.

- 4.2. Unless the Agreement or this Contract is terminated in accordance with their respective terms, this Contract shall expire on the later of

- 4.2.1. the expiry of the Initial Term of the Agreement; or,
- 4.2.2. the expiry of any Subsequent Term of the Agreement.

5. Consideration

- 5.1. In consideration of the mutual exchange of obligations set out herein, and having regard to the terms of the Agreement, the Parties agree to the terms of this Contract.

6. Data Protection

- 6.1. For the avoidance of doubt, under the Agreement the Service Provider owes the Service Recipient certain obligations, which the Service Recipient is entitled to enforce as a third party, and the provisions of this clause 6 supplement the provisions of the Agreement.
- 6.2. The Service Recipient shall own (or shall have the right to use) all right, title and interest in and to all of the Service Recipient Data.
- 6.3. In respect of Personal Data, the Service Recipient undertakes to comply with the provisions of the Data Protection Legislation in connection with the Service Recipient Data and any other Customer Data to which it has access.
- 6.4. The Parties acknowledge and agree that for the purposes of the Data Protection Legislation, the Service Recipient is the Controller, and the Service Provider is the Processor. The only processing that the Service Provider is authorised to do is recorded at Part D of the Agreement and replicated at Annex 1 for and on behalf of the Service Recipient and may not be determined by the Service Provider.
- 6.5. The Parties agree to take account of any guidance issued by the Information Commissioner or other relevant supervisory authority and the Customer may, on behalf of the Service Recipient and other Controllers, on not less than 30 Working Days' notice to the Service Provider amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

7. Confidentiality

- 7.1. The Parties undertake, except as provided below, to treat as confidential and keep secret the Confidential Information, with the same degree of care as it employs with regard to its own confidential information of a like nature and in any event in accordance with best current commercial security practices, provided that, this clause shall not extend to any information which was rightfully in the possession of either Party prior to the commencement of the negotiations leading to the Agreement or this Contract or which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause or any obligation on the Service Provider in the Agreement or this Contract).
- 7.2. A Party shall not without the prior written consent of the other relevant Party divulge any part of the Confidential Information to any person, other than the Customer, except:

- 7.2.1. to their own directors, officers, employees, servants, sub-contractors and agents and then only to those persons who need to know the same;
 - 7.2.2. to either Party's auditors, an officer of Inland Revenue, an officer of HM Revenue and Customs, a court of competent jurisdiction, governmental body or applicable regulatory authority and any other persons or bodies having a right duty or obligation to know the business of the other party and then only in pursuance of such right duty or obligation;
 - 7.2.3. where it must be disclosed pursuant to a statutory, legal or parliamentary obligation placed upon the party making the disclosure, including any requirements for disclosure by the Customer pursuant to Access to Information Legislation, save where an exemption applies; or
 - 7.2.4. to any person who is for the time being appointed by either Party to maintain the equipment on which the Software is for the time being used (in accordance with the terms of the Agreement and this Contract) and then only to the extent necessary to enable such person to properly maintain the equipment.
- 7.3. The Parties undertake to ensure that persons and bodies referred to in clause 7.2 above are made aware before the disclosure of any part of the Confidential Information that the same is confidential and that they owe a duty of confidence to the other Party.
- 7.4. The Service Recipients shall promptly notify the Service Provider if it becomes aware of any breach of confidence by any person to whom it divulges all or any part of the Confidential Information and shall give the Service Provider all reasonable assistance in connection with any proceedings which it may institute against such person for breach of confidence.

8. Intellectual Property

- 8.1. The Service Recipient warrants that all Intellectual Property Rights including but not limited to the Service Recipients' software, databases, graphics, diagrams, charts, sound and Service Recipient Data which shall be used and/or which is necessary for the Service Provider to access and use, is either the Service Recipient's property or is legally licensed to the Service Recipient to permit access and use by the Service Provider for the purpose of the IT Services.
- 8.2. The Service Recipient grants to the Service Provider a limited licence to use the Service Recipient's Foreground IPR for the purposes of the Agreement and this Contract.
- 8.3. All Intellectual Property Rights in the Service Recipient's software and Service Recipient Data created for and under this Agreement is the Service Recipient's and/or its licensors' Foreground IPR.
- 8.4. The Service Recipient grants to the Service Provider a limited, non-transferable, non-exclusive, royalty-free licence to use only such of the Service Recipient's and its licensors' Intellectual Property Rights as is required, solely to enable the Service Provider to deliver the IT System and to perform the IT Services.
- 8.5. Each Party recognises that the other Party's business relies upon the protection of its Intellectual Property Rights and that in the event of a breach or threatened breach of Intellectual Property Rights, the other Party shall be caused irreparable damage and such other Party may therefore be entitled to injunctive or other equitable relief to prevent a breach or threatened breach of its Intellectual Property Rights.
- 8.6. If a Party learns of any claim of infringement of the other Party's Intellectual Property Rights it shall promptly notify the other party.
- 8.7. In the event that, in the Service Provider's reasonable opinion, the use of the IT System is or may become the subject of an Intellectual Property Claim and the Service Provider cannot obtain for the Service Recipient the right to continue using the IT System which is the subject of the Intellectual Property Claim and cannot replace or modify the IT system which is the subject of the Intellectual Property Claim so it becomes non-infringing, the Service Recipient shall cease using the IT System which is the subject of the Intellectual Property Claim.

9. Co-operation with Service Provider

- 9.1. The Service Recipient acknowledges that its close involvement is essential to ensure that the IT Services successfully meet the Customer's requirements, and shall co-operate with the Service Provider's Representative, officers, employees and other independent consultants, and those of the Customer, whenever necessary or desirable in the performance of IT Services.
- 9.2. The Service Recipient shall appoint a Representative (identified at Schedule B) who is assigned to oversee the successful performance and delivery of the IT Services to the Service Recipient. The Service Recipient may change the identity of the Service Recipient's Representative or any of the details of the Service Recipient's Representative on written notice to the Customer and Service Provider.
- 9.3. If requested by the Service Provider and agreed by the Service Recipient to be necessary and expedient to the Service Provider's compliance with its obligations to the Service Recipient under the Agreement and this Contract, the Service Recipient shall provide a desk and wi-fi facilities for the use of the Service Provider on a licence-at-will basis.
- 9.4. In order for the Service Provider to be able to provide the Support Services to the Service Recipient, the Service Recipient shall:
 - 9.4.1. ensure that appropriate arrangements are put into place to allow remote access to the IT System, acceptable to the parties, or where remote access is not possible, to provide physical access to such premises of the Service Recipient as the Service Provider shall reasonably require, unless the instruction or requirement can be performed by the Service Recipient at the direction of the Service Provider;
 - 9.4.2. continue to maintain any IT System requirement in accordance with the minimum operating requirements from time to time as notified by the Service Provider or the owner thereof; and,
 - 9.4.3. ensure that staff are properly and adequately trained to a level of competence in relation to the IT System, in accordance with Service Provider's guidelines on training.

10. Access to Information

- 10.1. The Service Recipient acknowledges the Service Provider's request that the information identified at Part F of the Agreement be classified as reserved information under the Access to Information Legislation and not disclosable by the Service Recipient to third parties.

11. Dispute Resolution

- 11.1. If any dispute arises between the Parties in connection with the Agreement or this Contract, a director or other senior representative of each the Parties with authority to settle the dispute shall, within 14 days of a written request from one Party to the other, meet in good faith to resolve the dispute, together with a representative(s) of the Customer.
- 11.2. If the dispute is not wholly resolved at that meeting, the Parties agree to enter into mediation in good faith to settle such a dispute and will do so in accordance with the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure. The Customer shall be entitled to attend and participate in such mediation. Unless otherwise agreed between the parties within fourteen (14) days of notice of the dispute, the mediator will be nominated by CEDR. To initiate the mediation a Party must give an Alternative Dispute Resolution notice in writing ('ADR Notice') to the other Party, referring the dispute to mediation. A copy of the referral should be sent to CEDR.
- 11.3. Unless otherwise agreed, the mediation will start not later than twenty-eight (28) days after the date of the ADR Notice.
- 11.4. No Party may commence any arbitration or legal proceedings in relation to any dispute arising out of the Agreement or this Contract until it has attempted to settle the dispute by mediation and either the mediation has terminated, or the other Party has failed to participate in the mediation, provided that the right to issue proceedings is not prejudiced by a delay.

Liability

- 11.5. For the avoidance of doubt, the Parties' respective liability to the other shall be limited by and subject to the terms of the Agreement.
- 11.6. In particular, except as otherwise prohibited by law, the total liability of the Service Recipient to the Service Provider for any claims, losses, damages, costs and expenses arising under the Agreement or otherwise for any cause whatsoever, including under this Contract, shall be limited to the value of the monies paid to the Service Provider by the Customer under the Agreement.
- 11.7. The Parties acknowledge and agree that the limitations contained in this clause 12 and in the Agreement are commercially reasonable in the light of the nature of the IT Services, the identity of the Customer and Service Recipient and all the relevant circumstances relating to delivery of the IT Services.

12. Variation

- 12.1. This Contract may not be released, discharged, supplemented, interpreted, amended, varied or modified in any manner except in writing signed by a duly authorised officer or Representative of each of the Parties and the Customer.
- 12.2. Any change to this Contract shall be conducted in accordance with the provisions of the Agreement, including a Change Control Notice.

13. Termination

- 13.1. The Service Recipient shall be entitled to terminate this Contract for convenience at any time on thirty (30) days written notice to the Service Provider and the Customer.
- 13.2. The Service Recipient may terminate this Contract forthwith on giving notice in writing to the Service Provider and Customer:
 - 13.2.1. if the Service Provider breaches any obligation to the Service Recipient under any of the following provisions:
 - 13.2.1.1. clause 19 of the Agreement (Confidential Information);
 - 13.2.1.2. clause 20 of the Agreement (Customer Data and Data Protection);
 - 13.2.1.3. clause 21 of the Agreement (Freedom of Information); or,
 - 13.2.1.4. clause 22 of the Agreement (Security and Control).
- 13.3. On expiry or termination of this Contract for any reason the Service Provider shall:
 - 13.3.1. co-operate with the Service Recipient's requirements to return, destroy or delete (or to procure the return, destruction or deletion thereof) all:
 - 13.3.1.1. the Service Recipients' Confidential Information under its control or in its possession, unless and to the extent that such Confidential Information forms part of the Confidential Information of another service recipient;
 - 13.3.1.2. the Service Recipient Data, or media containing the Service Recipient Data or other materials provided by the Service Recipient, unless and to the extent that such Data or materials form part of the Data of another controller; and
 - 13.3.1.3. the Service Recipient owned property in the possession or control of the Service Provider or its sub-contractors, to the Service Recipient;
 - 13.4. deliver to the Customer a Certificate of Return, Destruction or Deletion signed and dated by a board director within 28 days of the contract expiry or termination.
- 13.5. Any termination of this Contract (howsoever occasioned) shall not affect any accrued rights or liabilities of either Party.

14. Survivorship

- 14.1. The provisions of any clause which by implication intended to come into or continue in force on or after termination shall by its nature be deemed to survive the termination of this Contract.

15. Agency, Partnership

- 15.1. This Agreement shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the Parties other than the contractual relationship expressly provided for in the Agreement and this Contract.

16. Notices

- 16.1. All notices under this Agreement shall be in writing.
- 16.2. Notices shall be deemed to have been duly given:
- 16.2.1. when delivered, if delivered by courier or other messenger (including registered mail) during normal business hours of the recipient; or
 - 16.2.2. when sent, if transmitted by fax or e-mail and a successful transmission report or return receipt is generated; or
 - 16.2.3. on the fifth (5th) business day following mailing, if mailed by national ordinary mail, postage prepaid; or
 - 16.2.4. each case addressed to the most recent address, e-mail address, or facsimile number notified to the other party.

17. Severance

- 17.1. If any provision of the Agreement or this Contract is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Agreement and/or this Contract and rendered ineffective as far as possible without modifying the remaining provisions of the Agreement and this Contract and shall not in any way affect any other circumstances of or the validity or enforcement of the Agreement or this Contract.

18. Assignment

- 18.1. This Contract is personal to the Service Provider and neither this Contract nor any rights, licences or obligations under it, may be assigned by the Service Provider, without the prior written approval of the Service Recipient and the Customer.

19. Duplicates

- 19.1. This Agreement shall be executed in duplicate, each of which shall be an original, and the duplicates shall together constitute one and the same agreement.

20. Costs and Expenses

- 20.1. Each party shall bear its own legal costs and other costs and expenses arising in connection with the drafting, negotiation, execution and registration (if applicable) of this Contract, and any other agreements the parties are required to enter into as specified in this Contract.

21. Law and jurisdiction

21.1. This Contract and all matters arising from it, including dispute resolutions, shall be governed by and construed in accordance with the Laws of England, and the Parties submit to the exclusive jurisdiction of the English Courts.

SCHEDULE A

Processing, Personal Data and Data Subjects

1. The Service Provider shall comply with any further written instructions with respect to processing by Customer.
2. Any such further instructions shall be incorporated into this Annex.

Subject matter of the processing	<p>The subject matter of the processing is the operation of Police CyberAlarm, which concerns the gathering, collation and analysis of data, including personal data primarily in the form of IP addresses, to identify suspicious cyber activity against UK public and private sector organisations with a view to understanding the nature and scale of the cyber threat to the UK, contributing to the prevention of and protection from such threat, and enabling its investigation, disruption and the taking of diversion/enforcement action.</p>
Duration of the processing	<p>The processing shall commence no sooner than the Commencement Date as specified in the Order Form and shall conclude upon the deletion/return of personal data following the expiry of the Initial Term, or any Subsequent Term or other permitted extension of the term of the Agreement or otherwise upon termination of the Agreement, in accordance with the requirements of Part A clause 14.2 of the Agreement and this Part D clause 1.4(e).</p> <p>It should be noted that not all categories of personal data will necessarily be processed from the outset of the duration of processing.</p>
Nature and purposes of the processing	<p>The purpose(s) of the processing are the law enforcement purposes, i.e., the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (see s31 Data Protection Act 2018).</p> <p>The nature of the processing activities includes the:</p> <ul style="list-style-type: none">• Collection;• Filtering;• Encryption;• Transmission;• Structuring;• Recording;• Storage;• Data matching/alignment;• Analysis;• Categorisation;• Scoring;• Retrieval;• Consultation;

	<ul style="list-style-type: none"> • Use; • Data sharing/disclosure; and, • Erasure/destruction. <p>Some of these activities may be conducted through machine learning.</p> <p>Other data is processed on the basis that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.</p>
Type of Personal Data	<p>The data processed will include personal data, including sensitive personal data and special category/criminal conviction and offence data.</p> <p>In respect of Police/law enforcement entity officers and staff:</p> <ul style="list-style-type: none"> • Name • .pnn/law enforcement entity email address • Force/law enforcement organisation • Rank/role • User credentials: email/password • Phone number • User group • Usage / logging data <p>Member organisation staff/their representatives:</p> <ul style="list-style-type: none"> • Name • Organisation (name & company registration number) • Role / Job title • Business Address • Region • Email address • Telephone number • Role • User credentials: username & password • Third party representative name • Third party representative email address • Payment data • Passcode • IP address • Usage data • Other personal data provided by member organisation staff/their representatives

Individuals suspected of involvement in suspicious activity:

- IP address
- Domain visited
- Sender email address
- Sender handle
- Recipient email address
- Email subject
- Email attachment filename
- Mail ID
- Location data:
 - Continent
 - Country
 - City
 - Postcode
 - Latitude
 - Longitude
 - Force area
 - Force region
 - Confidence in accuracy of location data
- ISP
- IP address host
- IP address owner
- Connection type, including whether a VPN or TOR is being used
- Device name
- Device ID
- Time zone
- Conduct data
- User agent
- Page sought to be accessed
- Page from which user was referred to page sought to be accessed
- Event ID
- Request type, i.e. to get/view, post etc
- Harm score of conduct
- Resolvability of conduct
- Postcode

	<p>Other users of member organisation's network, website, web apps, etc, including staff and third parties:</p> <ul style="list-style-type: none"> • IP address • Domain visited • Sender email address • Recipient email address • Email subject • Email attachment filename • Device name • Device ID • Time zone • Country • Conduct data <p>PCA website visitors:</p> <ul style="list-style-type: none"> • Visitor IP address; • Site from which user visited PCA website • PCA site usage.
Categories of Data Subject	<p>Categories of data subject are:</p> <ul style="list-style-type: none"> • Police/law enforcement entity officers and staff; • Member organisation staff/their representatives; • Individuals suspected of involvement in suspicious activity; • Other users of member organisation's network, website, web apps, etc, including staff and third parties; • Visitors to PCA website.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	<p>At the conclusion of the Initial Term or any Subsequent Term or other permitted extension of the Agreement or Contract or upon termination of the Contract, or at such time specified by the Customer prior to the conclusion of the Agreement to enable the efficient transfer of services to another provider, the Supplier shall promptly return all data to the Customer and/or relevant Service Recipient or transfer them directly to the new provider, and shall securely destroy all copies of data processed pursuant to the Agreement in accordance with any of the Customer's written instructions and in any event no later than thirty (30) days from the conclusion of the Agreement or Contract.</p>

Authorised Sub-Processors

For the purposes of the Agreement and this Contract, the Processor is entitled to engage the following sub-processors, subject to complying with the requirements of the Agreement Part D clauses 1.11-1.12 and on the basis that data will only be processed within the UK:

1.

s31 / s43(2)

2.

SCHEDULE B

Service Representative	Recipient's		
Customer's Representative	s40(2) ordinator	National Co-	s40(2)
Service Representative	Provider's	s40(2) Senior Systems Engineer (Programme Roll-out)	s40(2)

Signed on behalf of Pervade Software Limited

.....

Name:.....

Position:.....

Date:.....

Signed on behalf of [INSERT TITLE OF RELEVANT SERVICE RECIPIENT CHIEF/COMMISSIONER E.G. COMMISSIONER OF THE CITY OF LONDON POLICE]

.....

Name:.....

Position:.....

Date:.....