INTER-FORCE AGREEMENT

This Contract is made between:

1) [INSERT TITLE OF CHIEF CONSTABLE/COMMISSIONER] of [INSERT REGISTERED ADDRESS]

(the "Service Recipient");

2) The Mayor and Commonalty and Citizens of the City of London of Guildhall, PO BOX 270, London EC2P 2EJ (the "Customer"); and

3) The Commissioner of Police of the City of London (the 'Lead Controller')

(each a "Party" and 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 ("the Agreement").

AND WHEREAS the Service Recipient is granted certain rights and benefits under the Agreement

1. Interpretation

1.1.

1.1.1. CEDR Model Mediation Procedure means the mediation procedure established by the Centre for Effective Dispute Resolution.

1.1.2. **Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer** take the respective meanings given in The General Data Protection Regulation (Regulation (EU) 2016/679).

1.1.3. **Data Protection Impact Assessment** means an assessment of the impact of the envisaged processing on the protection of Personal Data s required by the Data Protection Legislation;

1.1.4. **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.

1.1.5. Data Subject Request means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access or control their personal data.

1.1.6. Intellectual Property Rights 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.

1.1.7. IT Services means 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 as set out in the Agreement;

1.1.8. **Law** means any 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 Controllers and/or their appointed Processors are bound to comply.

1.1.9. Member Badge means the Police CyberAlarm branding which a Member Organisation is authorised to utilise in accordance with the Member Orgnisation Agreement.

1.1.10. Member Organisation means an entity which registers for Police CyberAlarm and enters into the Member Organisation Agreement with a Service Recipient.

1.1.11. Member Organisation Agreement means the agreement entered into between the Service Recipient and a Member Organisation in connection with the provision of Police CyberAlarm.

1.1.12. National Police Chiefs Council's Cybercrime Programme means the programme of work undertaken on behalf of the Home Office for the benefit of policing hosted by the City of London Police.

1.1.13. Police CyberAlarm means the system and services procured pursuant to the Agreement as may be modified or replaced from time to time.

1.1.14. Police CyberAlarm Reports means the reports issued by or on behalf of the Service Recipient to Member Organisations analysing the Data provided by the Member Organisation to the Force.

1.1.15. Project Lead means S.23(1) **,** or such other individual who may be appointed from time to time and notified to the Service Recipient by the Lead Controller.

1.1.16. Service Provider Agreement means the contract entered into between the Service Recipient and the Service Provider in connection with the provision of the IT Services pursuant to the Agreement.

1.1.17. Territory means the United Kingdom of Great Britain and Northern Ireland.

2. Term

2.1. This Contract shall commence on the date it is signed by the Service Recipient.

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

2.2.1. the expiry of the Initial Term of the Agreement; or,

2.2.2. the expiry of any Subsequent Term of the Agreement.

3. Consideration

3.1. 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.

4. Agency, Partnership

4.1. This Contract 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 Contract.

5. Intellectual Property Rights

5.1. The Service Recipient acknowledges and agrees that all Intellectual Property Rights in the Police CyberAlarm services, including but not limited to the software, logo, website, services, system and any documentation relating to Police CyberAlarm, including Police CyberAlarm Reports, are and shall remain the property of the Customer and/or its licensors.

5.2. The Customer grants to the Service Recipient within the jurisdiction for the Term of this Contract and subject to, and in accordance with the terms of this Agreement, a limited, non-exclusive and royalty-free licence to:

5.2.1. use such of the Customer's Intellectual Property Rights as are necessary to enable the Service Recipient to utilise the Police CyberAlarm services in accordance with the terms of the Agreement and this Contract;

5.2.2. sub-licence such of the Customer's Intellectual Property Rights as are necessary to enable relevant Member Organisations to utilise the Police CyberAlarm services in accordance with the terms of the Agreement, this Contract and the Member Organisation Agreement;

5.2.3. use such of the Customer's Intellectual Property Rights as are necessary to promote the Police CyberAlarm services, subject to clause 15;

5.2.4. sub-licence such Intellectual Property Rights as are necessary in the Member Badge to relevant Member Organisations, subject to such limitations and restrictions as may be set out in the Member Organisation Agreement;

5.2.5. copy, publish, distribute, transmit and adapt the information contained within any Police CyberAlarm Report for non-commercial purposes limited to the fulfilment of their law enforcement obligations within the relevant force area, and to sub-licence such rights only to relevant Member Organisations solely for their internal use and provided that the Member Organisation acknowledges the source of the information.

5.3. Other than as expressly provided for in this Contract, the Service Recipient shall have no rights to use the Customer's or Lead Controller's names, logos, trademarks or other Intellectual Property Rights without the Customer's or Lead Controller's prior written approval as appropriate.

5.4. The Parties acknowledge and agree that the all Intellectual Property Rights in the Service Recipient Data are and shall remain the property of the relevant Service Recipient and/or its licensors.

5.5. The Service Recipient grants to the Customer and the Lead Controller a perpetual, non-revocable, transferable and sub-licensable worldwide licence of the Intellectual Property Rights in the Service Recipient Data.

5.6. The Parties shall:

5.6.1. only make use of the Intellectual Property Rights for the purposes and in the manner authorised in this Contract;

5.6.2. comply with all regulations and practices in force or use in the Territory to safeguard the Intellectual Property Rights of the Parties and/or their licensors;

5.6.3. not do or omit to do anything to diminish the Intellectual Property Rights of the Parties or their licensors, nor assist any other person to do so, whether directly or indirectly.

5.7. The Parties acknowledge and agree that the exercise of the rights and licences granted under this Contract are subject to all applicable laws, enactments, regulations and other similar instruments in the Territory, and the Parties understand and agree that they shall at all times be solely liable and responsible for such due observance and performance.

5.8. If a Party learns of any claim of infringement of another Party's Intellectual Property Rights in the context of Police CyberAlarm, it shall promptly notify the relevant Party and the Project Lead on behalf of the Customer and the Lead Controller. The Parties shall provide reasonable assistance to each other to assist the relevant Party in taking proceedings or any other actions the relevant Party may reasonably take to terminate or prevent any such claim.

6. Data Protection Compliance

6.1. The Parties shall each comply with and shall be solely responsible for compliance with their respective obligations under the Data Protection Legislation and other applicable Law in connection with the processing of personal data in the context of Police CyberAlarm, and shall establish mechanisms, including auditing measures, to ensure their respective compliance with the Data Protection Legislation.

6.2. The Parties shall notify any particulars as may be appropriate to the Information Commissioner, as the relevant Supervisory Authority in the Territory, or such other Supervisory Authority as required by the Data Protection Legislation. Each Party declares that it has at the date of entering into this Contract and shall maintain throughout the Term such valid registrations and/or has paid such fees as are required by any relevant Supervisory Authority which, at the time data sharing is expected to commence, shall reflect data sharing pursuant to this Agreement, unless an exemption applies.

6.3. The Parties agree and declare that the processing of Personal Data in the context of this Contract and Police CyberAlarm is necessary and proportionate having regard to the purpose(s) of processing, which are the law enforcement purposes, i.e. the prevention, investigation, detection and/or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and in particular cybercrime ('the Purpose'), and that the processing is necessary for the performance of a task carried out for the law enforcement purposes, which could not be achieved without recourse to the processing of Personal Data.

6.4. The Service Recipient shall be the Data Controller in respect of Personal Data collected from Member Organisations registered to that Service Recipient's force area and processed on the Service Recipient's behalf by the Service Provider pursuant to the Service Provider Agreement.

6.5. Each party shall remain a Data Controller of any Personal Data which they each process for their own business purposes further to the Agreement, this Contract and/or the Service Provider Agreement.

6.6. Without prejudice to the Parties' respective obligations under the Data Protection Legislation and clause 6.1, the Lead Controller shall:

6.6.1. prepare and make available such transparency information as is required by the Data Protection Legislation in connection with the operation of Police CyberAlarm on its website;

6.6.2. conduct a Data Protection Impact Assessment in respect of the processing of Personal Data in the context of Police CyberAlarm prior to the commencement of processing and shall conduct periodic reviews of its adequacy;

6.6.3. prepare and implement a data retention policy in relation to Personal Data stored on Police CyberAlarm;

6.6.4. conduct a review of the Police CyberAlarm legal and compliance documentation at least annually, and shall amend and/or make recommendations as to any amendments considered to be appropriate to maintain or secure compliance with the Law;

6.6.5. provide regular reports concerning the operation of Police CyberAlarm to the NPCC Cybercrime Programme Board or such other governance mechanism as may be established in accordance with clause 17.

6.7. Without prejudice to the Parties respective obligations under the Data Protection Legislation and clause 6.1, the Parties agree that, for the purpose of enabling Data Subjects to exercise their rights under the Data Protection Legislation, the Lead Controller shall arrange for and publicise on the Police CyberAlarm website a single point of contact to which Data Subjects may submit a Data Subject Request.

6.8. Where the Lead Controller receives a Data Subject Request relating to Personal Data processed in the context of Police CyberAlarm under the arrangement established pursuant to clause 6.7 above, the Lead Controller shall notify any relevant Service Recipient and shall co-ordinate the identification and collation of any Personal Data liable to be disclosed.

6.9. Where a Service Recipient receives a Data Subject Request relating to Personal Data processed in the context of Police CyberAlarm, the Party shall notify the Project Lead on behalf of the Lead Controller, who shall co-ordinate the identification and collation of any Personal Data liable to be disclosed, and the relevant Service Recipients shall be informed.

6.10. Where a Service Recipient determines that It is obliged to rectify, erase or restrict Personal Data processed in the context of this Agreement, it shall promptly notify the Project Lead.

6.11. The Parties shall each co-operate and provide reasonable assistance to the other Parties in connection with complying with their respective obligations under the Data Protection Legislation.

6.12. In the event that the Service Recipient becomes aware of any unauthorised access to or use Personal Data processed in the context of Police CyberAlarm or any other security incident affecting its network and information systems that could potentially affect the operation of Police CyberAlarm, it shall promptly notify the Project Lead.

6.13. In the event that the Service Recipient becomes aware of any potentially unlawful processing of Personal Data in the context of Police CyberAlarm, or of any deficiencies in compliance with the requirements of the Data Protection Legislation in relation to the processing of Personal Data in the context of Police CyberAlarm, it shall promptly notify the Project Lead.

6.14. The Parties agree to take account of any guidance issued by any relevant Supervisory Authority relevant to their obligations under this Contract. The Parties may agree to, or on not less than thirty (30) days' notice the Lead Controller may unilaterally, amend this Agreement to ensure that it complies with any guidance issued by the Supervisory Authority or other Law.

7. Personal Data Sharing

7.1. The Service Recipient agrees to share with the Lead Controller the Personal Data collected from Member Organisations registered to that Service Recipient's force area and processed on the Service Recipient's behalf by the Service Provider pursuant to the Service Provider Agreement, as identified at Schedule A of the Service Provider Agreement.

7.2. The Lead Controller shall only process the Personal Data shared by the Service Recipient pursuant to clause 7.1 for the Purpose, or any other compatible or lawful purpose.

7.3. The Service Recipient acknowledges and agrees that the processing to be conducted by the Lead Controller in accordance with clause 7.2 shall include the sharing of Personal Data with other Service Recipients for the Purpose where necessary and proportionate to do so.

7.4. The Parties acknowledge and agree that the sharing of Personal Data from the Service Recipient to the Lead Controller and from the Lead Controller to other Service Recipients involves a Data Controller to Data Controller transfer of Personal Data.

7.5. The Parties acknowledge and agree that the sharing of Personal Data pursuant to clauses 7.1 and 7.4 above shall take place on an ongoing, routine basis, by granting access to relevant individuals to the Personal Data on the secure Police CyberAlarm platform.

8. Confidentiality

8.1. Except to the extent required by law or any legal or regulatory authority of competent jurisdiction or except with the other Parties' consent as appropriate no Party shall at any time

disclose to any person (other than their professional advisers, employees, contractors, officers, representatives, sub-contractors volunteers or other parties with a reasonable need to know) the terms of this Contract or any trade secret or other confidential information relating to Police CyberAlarm or make any use of such information other than to the extent necessary for the purpose of exercising or performing its rights and obligations under, or in connection with, this Contract, The Agreement and/or the Service Provider Agreement.

8.2. Where a disclosure is required by law or any governmental or regulatory authority, or by any court or other authority of competent jurisdiction, the Party required to make the announcement shall promptly notify the other relevant Parties. The Party concerned shall make all reasonable attempts to agree the contents, manner and timing of the announcement before making it.

9. Liability

9.1. For the avoidance of doubt, neither the Customer nor Lead Controller are liable to the Service Recipient in connection with the delivery of the IT Services and the Service Recipient's sole remedy shall lie with the Service Provider as limited by and subject to the terms of the Agreement.

9.2. Neither Party excludes or limits liability to the other Party for:

9.2.1. death or personal injury caused by its negligence, or that of its employees, agents or sub-contractors;

9.2.2. bribery, fraud or fraudulent misrepresentation by it or its employees;

9.2.3. breach of any obligations implied by section 2 of the Supply of Goods and Services Act 1982; or,

9.2.4. any other matter which, by Law, may not be excluded or limited.

9.3. In no event shall the Parties or any of them 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.

9.4. No Party may benefit from the limitations and exclusions set out in this clause 9 in respect of any liability arising from its deliberate default. Nor may a Party benefit from any indemnity in this Contract to the extent that a claim under it results from the Indemnified Party's negligence or wilful misconduct.

9.5. Subject to clauses 9.3 and 9.4 above, each Party to this Contract agrees to indemnify the other Parties against any costs, damages and expenses incurred in connection with, and arising from, legal claims (of whatever nature) for which the indemnifying Party is liable due to its failure to adhere to the Data Protection Legislation or to comply with the obligations in clauses 5 or 8 of this Contract.

9.6. The Parties acknowledge and agree that the limitations contained in this clause 9 are commercially reasonable in light of the nature of the arrangements between the Parties, the funding arrangements for Police CyberAlarm, the contractual arrangements in place between

the Service Recipients and Member Organisations, the Parties' respective identities and all the relevant circumstances relating to the Contract.

10. **Disputes with the Service Provider**

10.1. Prior to exercising any right extended to the Service Recipient against the Service Provider by the Agreement, the Service Recipient shall provide prior written notice to the Project Lead on behalf of the Customer and Lead Controller and shall liaise and co-operate with the Lead Controller, and other Service Recipients, to co-ordinate the exercise of rights affecting the Parties and other Service Recipients.

10.2. The Service Recipient shall consider in good faith and, unless the Service Recipient provides a written justification to the Project Lead for acting to the contrary, shall adopt any proposals made by the Project Lead in relation to the exercise of any rights under the Agreement with a view to ensuring that the Parties and other affected Service Recipients achieve an equitable resolution to any dispute with the Service Provider.

11. **International Liaison**

11.1. The Parties acknowledge and agree that the Lead Controller shall act as the single point of contact in respect of any proposal to or request for the disclosure of Personal Data gathered or processed in the context of Police CyberAlarm to a third country or international organisation.

11.2. The Service Recipient shall refer any proposal to or request for the disclosure of Personal Data gathered or processed in the context of Police CyberAlarm to a third country or international organisation to the Lead Controller to consider and determine the response to.

11.3. The Lead Controller shall maintain records relating to its decision making and any transfer of personal data pursuant to clause 11.1

12. **Support services and fault escalation**

12.1. In the event of a Fault affecting a Service Recipient, this shall be reported by the Service Recipient to the Service Provider in accordance with the provisions of Part B of the Agreement.

12.2. In the event that the Service Provider and Service Recipient are unable to agree a Fault classification in accordance with the provisions of Part B of the Agreement, the Service Recipient shall inform the Project Lead, who shall investigate and, if the Project Lead disagrees with the designation of the Fault classification by the Service Provider shall escalate the designation in accordance with the provisions of Part B of the Agreement.

13. **Complaints from Member Organisations and members of the public and inquiries by regulators**

13.1. In the event that the Service Recipient receives a complaint or threatened claim from a Member Organisation or member of the public concerning Police Cyber Alarm, or is contacted by a regulatory body regarding the operation of Police CyberAlarm, the Service Recipient shall:

13.1.1. promptly notify the Project Lead on behalf of the Customer and Lead Controller;

13.1.2. consult the Project Lead on behalf of the Customer and Lead Controller in relation to the timing and content of any response;

13.1.3. consider in good faith any proposals made by the Project Lead on behalf of the Customer and Lead Controller in relation to the timing and content of any response.

13.2. The Parties' respective obligations to notify the other under clause 7.13 above shall include the provision to the other Party of full details and copies of the complaint, communication or request, and the prompt provision of such further information in phases, as details become available, and such assistance as may reasonably be required in responding to any communication from a Supervisory Authority or other regulatory authority or third party.

14. Access to Information Rights

14.1. The Parties acknowledge that they may each be 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.

14.2. Without prejudice to clause 14.1 or to the Parties' respective obligations, the Parties agree to:

14.2.1. Promptly inform the Project Lead on behalf of the Customer and Lead Controller of any request to access information related to Police CyberAlarm;

14.2.2. consult the Project Lead on behalf of the Customer and Lead Controller in relation to the timing and content of any response;

14.2.3. consider in good faith any proposals made by the Project Lead on behalf of the Customer and Lead Controller in relation to the timing and content of any response.

15. Publicity, Reputation & Legal Obligations

15.1. The Lead Controller shall develop and maintain a website for the purpose of publicising Police CyberAlarm and shall administer any enquiries relating to Police CyberAlarm.

15.2. The Lead Controller shall take such steps as it considers appropriate in order to publicise Police CyberAlarm to relevant entities, which may include engaging third parties to publicise Police CyberAlarm.

15.3. No Service Recipient shall issue or make any public announcement regarding the Agreement, this Contract or Police CyberAlarm unless prior written consent has been obtained from the Project Lead on behalf of the Customer and Lead Controller.

15.4. The Parties will not act in any way which causes or may reasonably be expected to cause, damage to the reputation of another Party or which otherwise causes another Party to breach any of its legal obligations.

16. Commercialisation

16.1. The Service Recipient acknowledges and agrees that the Customer and/or the Lead Controller may take steps to commercialise Police CyberAlarm, or any part of it, and/or the Service Recipient Data for the purpose(s) of funding Police CyberAlarm and/or the National Police Chiefs Council's Cybercrime Programme and the Service Recipient shall not be entitled to any benefit of such commercialisation.

17. Governance & oversight

17.1. Governance in respect of Police CyberAlarm shall be undertaken by the NPCC Cyber Crime Programme Board, chaired by the Assistant Commissioner for Economic and Cybercrime, City of London Police or such individual as may be appointed by them, or any governance mechanism as may be established from time to time.

18. Dispute Resolution

18.1. The Parties shall work on the basis that any disputes arising in connection with this Contract will be settled amicably and in good faith.

18.2. Any dispute shall be referred, in the first instance to the Project Lead and may thereafter be escalated if necessary to:

18.2.1. The National Police Chiefs' Council's National Cybercrime Programme Lead; and,

18.2.2. the NPCC Cyber Crime Programme Board

18.3. In the event that any dispute has not been resolved following the escalated referral process in clause 18.2, the Parties agree to enter into mediation in good faith to settle such a dispute and will do so in accordance with the CEDR Model Mediation Procedure. Unless otherwise agreed between the Parties within 14 days of notice of the dispute, the mediator will be nominated by CEDR.

19. Assignment and other dealings

19.1. The Service Recipient shall not assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any or all of their rights and obligations under this Contract (or any other document referred to in it) without the prior written consent of the Customer.

20. Variation and waiver

20.1. 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.

20.2. A waiver of any right or remedy under this Contract or by law is only effective if it is given in writing and is signed by the Party waiving such right or remedy. Any such waiver shall apply only to the circumstances for which it is given and shall not be deemed a waiver of any subsequent breach or default.

20.3. A failure or delay by any party to exercise any right or remedy provided under this Contract or by law shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy.

20.4. No single or partial exercise of any right or remedy provided under this Contract or by law shall prevent or restrict the further exercise of that or any other right or remedy.

20.5. A Party that waives a right or remedy provided under this Contract or by law in relation to one Party, or takes or fails to take any action against that Party, does not affect its rights or remedies in relation to any other Party.

21. Severance

21.1. If any provision or part-provision of this Contract is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this Contract.

22. Termination

22.1. Subject to clause 22.2, the Parties may terminate this Contract prior to the expiry of the Initial Term of the Agreement or any Subsequent Term of the Agreement on thirty (30) days' written notice to the other Parties.

22.2. In the event that this Contract is terminated pursuant to clause 22.1, the Service Recipient shall from expiry of the notice period cease to be entitled to the receipt of the IT Services under the Agreement and the Project Lead shall, unless determined at the sole discretion of the Customer and Lead Controller, work with the Service Provider to remove the Service Recipients access to the IT Services .

22.3. On termination of this Contract, the following clauses shall continue in force:

22.3.1. Clause 6 (Data Protection Compliance);
22.3.2. Clauses 7.2 – 7.4;
22.3.3. Clause 8 (Confidentiality);
22.3.4. Clause 9 (Liability);
22.3.5. Clause 10 (Disputes with the Service Provider);

22.3.6. Clause 11 (International Liaison);
22.3.7. Clause 13 (Complaints from Member Organisations and members of the public and inquiries by regulators);
22.3.8. Clause 14 (Access to information rights);
22.3.9. Clause 15 (Publicity, Reputation & Legal Obligations);
22.3.10. Clause 16 (Commercialisation);
22.3.11. Clause 17 (Third Parties);
22.3.12. Clause 19 (Dispute Resolution);
22.3.13. Clause 20 (Assignment & Other Dealings);
22.3.14. Clause 28 (Governing Law & Jurisdiction).

22.4. Termination of this Contract shall not affect any rights, remedies, obligations or liabilities of any of the Parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the Contract which existed at or before the date of termination.

22.5. In the event that the Service Recipient terminates this Contract prior to the expiry of the Initial Term or any Subsequent Term of the Agreement, the Service Recipient shall provide reasonable assistance to the Lead Controller in the event that the Lead Controller considers it desirable to transfer the Member Organisations in the Service Recipient's force area to another Service Recipient in order to permit the Member Organisations to continue to subscribe to Police CyberAlarm.

23. Notices

23.1. All notices under this Agreement shall be in writing.

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

24. Third party rights

A person who is not a party to this Contract shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Contract.

25. Costs and expenses

Except as expressly provided in this agreement, each party shall pay their own costs and expenses incurred in connection with the negotiation, preparation, execution and performance of this agreement (and any documents referred to in it).

26. Counterparts

This Contract may be executed in any number of counterparts, each of which when executed and delivered shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.

27. Entire Agreement

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.

28. Governing law & jurisdiction

This Contract and all matters arising from it, including dispute resolution, 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.

Signed on behalf of The Mayor and Commonalty and Citizens of the City of London

……

Name:……..

Position:……

Date:……...

Signed on behalf of the Commissioner of the City of London Police

……..……

Name:……..

Position:……

Date:……...

Signed on behalf of [INSERT TITLE OF RELEVANT SERVICE RECIPIENT]

……..…….....

Name:……..

Position:……

Date:……