POLICE CYBERALARM

MEMBER ORGANISATION AGREEMENT

1. The Parties

1.1. The Parties to this Agreement are:

1.1.1. The UK territorial police force referring the Member Organisation to Police CyberAlarm (hereinafter referred to as 'the Force'); and,

1.1.2. The company or other entity registered to receive Police CyberAlarm (hereinafter referred to as 'the Member Organisation'),

together, 'the Parties'.

2. Definitions

2.1. The following words and phrases used in this Contract shall have the following meanings except where the context otherwise requires.

2.1.1. In this Agreement, the expressions **Data, Controller, Data Subject, Processor, Processing, Personal Data, Personal Data Breach, Pseudonymisation** and **Supervisory Authority** have the same meaning as in Article 4 of GDPR, subject to any modification introduced by the Data Protection Act 2018.

2.1.2. **Data Protection Legislation** means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy and (iii) all applicable Law about the processing of personal data and privacy.

2.1.3. **Special Categories of Personal Data** has the same meaning as in Article 9 of the GDPR, subject to any modification introduced by the Data Protection Act 2018.

2.1.4. **Criminal Conviction and Offence Data** has the same meaning as in section 11 Data Protection Act 2018.

2.1.5. **GDPR** means the General Data Protection Regulation (Regulation (EU) 2016/679).

2.1.6. **LED** means the Law Enforcement Directive (Directive (EU) 2016/680).

2.1.7. **Data Loss Event** means any event that results, or may result, in unauthorised access to Personal Data processed pursuant to this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach.

2.1.8. **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.

2.1.9. **Police Data** means any Data including Personal Data, Special Categories of Personal Data and Criminal Conviction and Offence Data, collected by the Force and processed by it as identified in this Agreement.

2.1.10. **Police CyberAlarm Reports** means the reports issued by or on behalf of the Force to the Member Organisation analysing the Data provided by the Member Organisation to the Force.

2.1.11. **Agreement** means this Agreement together with its schedules and all other documents attached to or referred to as forming part of this Agreement, including information submitted by the Member Organisation when registering and submitting its electronic signature and the order confirmation.

2.1.12. **Protective Measures** means appropriate technical and organisational measures to protect the security, and in particular the confidentiality, integrity and availability of Personal Data, which may include: encryption, hashing, 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 such measures adopted.

2.1.13. **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.

2.1.14. **Confidential Information** means all Police Data, Police CyberAlarm Reports, Police CyberAlarm user credentials and access code, and any other information identified by the Parties as being confidential in nature and which is not legitimately in the public domain.

2.1.15. **Police CyberAlarm** means the services made available by the Force to the Member Organisation which may comprise of one or more of the following services (which may be amended from time to time) which the Member Organisation may elect to receive one or more of as part of the registration and as detailed in the confirmation: (i) vulnerability scanning of the Member Organisation's external facing networks, website and applications; (ii) the analysis of network based anti-virus log data; (iii) the analysis of network based intrusion detection log data; (iv) the analysis of network based spam logs; (v) the analysis of external network traffic (firewall) logs; (vi) the analysis of web server logs; (vii) the analysis of content delivery network logs; and (viii) the provision of reporting to Member Organisations regarding the vulnerability scanning and analysis undertaken in relation to the services elected to be received by the Member Organisation (the Police CyberAlarm Reports).

2.1.16. **Member Organisation Data** means Data, including Personal Data, Special Categories of Personal Data and Criminal Conviction and Offence Data, collected by the Member Organisation as a Data Controller and which the Member Organisation makes available for sharing with the Force for the purpose of Police CyberAlarm.

2.1.17. **Intellectual Property Rights** means patents, utility models, rights to inventions, copyright and neighbouring and related rights, moral rights, trade marks and service marks, business names and domain names, rights in get-up and trade dress, goodwill and the right to sue for passing off or unfair competition, rights in designs, rights in computer software, database rights, rights to use, and protect the confidentiality of, Confidential Information (including know-how and trade secrets) and all other intellectual property rights relating to Police CyberAlarm, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

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

2.1.19. **Member Badge** means the Police CyberAlarm branding which the Member Organisation is authorised to utilise in accordance with this Agreement, as identified in the Branding Guidelines.

2.1.20. **Branding Guidelines** means the Force's conditions with regard to the depiction of the Member Badge and promotional and advertising material containing the Member Badge as set out on the Police CyberAlarm website, as may be updated from time to time.

2.1.21. **Police CyberAlarm website** means https://cyberalarm.police.uk/.

3. Interpretation

3.1. Headings are inserted for convenience only and shall not affect the construction or interpretation of this Agreement and, unless otherwise stated, references to clauses and schedules are references to the clauses of and schedules to this Agreement;

3.2. 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.

3.3. 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.

4. Consideration

4.1. In consideration of the mutual exchange of obligations set out herein, the Parties agree to the terms of this Agreement.

5. Formation of contract, Commencement, Term, Variation & Termination

5.1. The Member Organisation enters into this Agreement by registering its details, selecting the elements of Police CyberAlarm to receive and submitting its electronic signature via the Police CyberAlarm website.

5.2. Where an individual enters into this Agreement on behalf of a company or other entity, that individual warrants and represents that they have the requisite authority to enter into this Agreement on behalf of the Member Organisation and to bind the Member Organisation to its terms.

5.3. This Agreement shall commence upon submission of an electronic signature by or on behalf of the Member Organisation and shall operate until either Party wishes to exit from this Agreement (the 'Term').

5.4. If there is any conflict or ambiguity between the terms of the documents forming part of the Agreement, a term contained in this Agreement shall have priority over a term in the order form, which shall have priority over a term in any schedule.

5.5. The Force shall be entitled, on not less than thirty (30) days' written notice to the Member Organisation, to vary the terms of this Agreement, including to take account of any changes to the delivery of Police CyberAlarm.

5.6. Subject to clause 5.5 above and clause 7.16 below, no variation to the Agreement shall be effective without the written consent of the Parties.

5.7. In the event that the Member Organisation wishes to exit from this Agreement, the Member Organisation shall uninstall the relevant software from their system, which shall cease the sharing of further Personal Data pursuant to this Agreement.

5.8. The Force shall be entitled to terminate this Agreement at any time for any reason, and shall do so by removing the Member Organisation's access to Police CyberAlarm and ceasing to collect further Personal Data pursuant to this Agreement.

5.9. Clauses 6.10, 7.12, 7.13, 8.1, and 10.1 shall survive the termination of this Agreement.

6. Provision of Police CyberAlarm

6.1. The Force grants the Member Organisation the non-exclusive and non-transferable right to access and use Police CyberAlarm within the Territory, subject to the terms of this Agreement.

6.2. Police CyberAlarm is made available to the Member Organisation "as available" and "as is" without warranty of any kind, express or implied, including but not limited to warranties of availability, performance, merchantability, fitness for a particular purpose, accuracy, omissions, completeness, currency, uninterrupted service and delays. Without limitation, the Force does not guarantee the identification of any or all security vulnerabilities that may be present on a Member Organisation's network, nor does it guarantee the reporting of any such vulnerabilities to the Member Organisation, nor does it guarantee the timeliness of any reporting.

6.3. The Force excludes all implied conditions, warranties, representations or other terms that may apply in connection with Police CyberAlarm.

6.4. Police CyberAlarm may be modified from time to time, including by adding or deleting features and functionality, or temporarily or permanently withdrawn from service without notice to Member Organisations. Any additional services will only be provided to the Member

Organisation where the Member Organisation agrees to the receipt of such services and any associated data sharing.

6.5. The Member Organisation shall be solely responsible for configuring its information technology systems, network, devices, computer programmes and platform for use with Police CyberAlarm and the Force accepts no liability in connection with the Member Organisation's inability or failure to so configure.

6.6. The Member Organisation is solely responsible for ensuring that its use of Police CyberAlarm and its processing of Member Organisation Data, including the collection, storage and transfer of Member Organisation Data to the Force, complies with all applicable Law including, but not limited to, the Human Rights Act 1998, The Investigatory Powers Act 2016, The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 (SI 2018/356) and, the Data Protection Legislation.

6.7. The Member Organisation is and shall remain solely responsible for maintaining the security and integrity of its own systems, network and devices, and remedying any vulnerabilities identified by Police CyberAlarm.

6.8. The Member Organisation is responsible for ensuring that all log in information issued to it by or on behalf of the Force in connection with Police CyberAlarm, including username, password and access code, are kept secure and confidential. The Member Organisation must promptly inform the Force in the event of any confidentiality breach or unauthorised use of any Police CyberAlarm user credentials or access codes.

6.9. Without prejudice to any other rights or remedies to which the Force may be entitled whether under this Agreement or at common law, the Force reserves the right to disable the Member Organisation's Police CyberAlarm user credentials or access codes and/or to withdraw the Member Organisation's access to Police CyberAlarm without notice in the event that it believes that the Member Organisation has failed to comply with any of the provisions of the Agreement. Such action will terminate the Agreement in accordance with clause 5.3.

6.10. The Member Organisation must not and must ensure that its directors, officers, employees, servants and agents do not:

6.10.1. attempt to undermine the security or integrity of Police CyberAlarm's systems, networks, devices or the Police Data;

6.10.2. use, or misuse, Police CyberAlarm in a manner which may impair its functionality, or that of the systems, network and devices used to deliver Police CyberAlarm, or the ability of other Member Organisations to use Police CyberAlarm;

6.10.3. attempt to gain access to Police CyberAlarm, its systems, network, devices, and any Police Data or other information transferred to or stored as part of Police CyberAlarm in any manner other than as expressly authorised in this Agreement during its Term;

6.10.4. attack Police CyberAlarm, its systems, network and devices, via a denial-of-service attack or a distributed denial-of service attack;

6.10.5. attempt to modify, copy, adapt, reproduce, disassemble, decompile or reverse engineer any code relating to Police CyberAlarm or any other part of Police CyberAlarm except as is strictly necessary for normal operation during the Term;

6.10.6. sell, resell, license, sublicense, distribute or otherwise make available Police CyberAlarm to any third party.

6.11. The Member Organisation authorises the Force and/or its representatives to install Police CyberAlarm and its constituent parts on the Member Organisation's network, systems and devices in any form howsoever comprising hardware, software or otherwise, and grants access to such programs and data as are necessary for the delivery of Police CyberAlarm.

7. Data Sharing

7.1. The use and disclosure of any Personal Data for the Purpose shall be in accordance with the obligations imposed upon the Parties to this Agreement by the Data Protection Legislation, the Human Rights Act 1998 and other applicable Law.

7.2. The Parties declare that the processing of Personal Data in the context of this Agreement 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'), which could not be achieved without recourse to the processing of Personal Data.

7.3. The Member Organisation will share with the Force the Member Organisation Data, as are relevant to the Police CyberAlarm services requested by the Member Organisation at the point of registration or subsequently and as detailed in the order confirmation. Details of the types of Personal Data processed in connection with each of the Police CyberAlarm services is described in the Member Organisation Log Data Schedule, which may be updated from time to time and is made available on the Police CyberAlarm website.

7.4. The Force will share with the Member Organisation such Police Data as are relevant to the analysis and reporting to the Member Organisation of Member Organisation Data provided to the Force as described at clause 7.3 above.

7.5. The Parties undertake to comply with the provisions of the Data Protection Legislation in connection with the processing of Personal Data in the context of this Agreement at all times during its Term.

7.6. Without prejudice to the generality of clause 7.5 above, the Member Organisation warrants and represents:

7.6.1. that the that the Purpose is consistent with the original purpose(s) of the data collection;

7.6.2. that it has legitimate grounds under the Data Protection Legislation to process the Personal Data as envisaged by this Agreement and the right to share the Member Organisation Data with the Force for the Purpose;

7.6.3. that its lawful basis for processing Personal Data in the context of this Agreement is that it is necessary for the purposes of its legitimate interests and those of the Force and society at large, and that such interests are not overridden by the interests or fundamental rights and freedoms of any affected Data Subject which require protection of personal data;

7.6.4. that its lawful basis for processing Personal Data comprising Criminal Conviction and Offence Data in the context of this Agreement is that it is necessary for the purposes of

the prevention or detection of an unlawful act, which must be carried out without the consent of the data subject so as not to prejudice those purposes, and is necessary for reasons of substantial public interest and involves the disclosure of personal data to a competent authority within the meaning of the Data Protection Legislation;

7.6.5. that it shall, in respect of Member Organisation Data to be shared pursuant to this Agreement, ensure that it makes available clear and sufficient information to Data Subjects as required by the Law, including the Data Protection Legislation and The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 (SI 2018/356); and,

7.6.6. that it shall, in respect of Personal Data submitted by the Member Organisation to the Force in the course of registering to receive Police CyberAlarm, promptly provide to any of its directors, officers, employees, agents, consultants, contractors or other individuals affected by the processing of such Personal Data the Police CyberAlarm Privacy Policy as published on the Police CyberAlarm website.

7.7. The Force warrants and represents that:

7.7.1. its lawful basis for the processing of Personal Data in the context of this Agreement is that it is processing for the law enforcement purposes and the processing is necessary for the performance of a task carried out for the law enforcement purposes;

7.7.2. it shall only process Personal Data in the context of this Agreement for the law enforcement purposes, unless any other processing is authorised by Law;

7.7.3. it shall, in respect of Personal Data to be shared pursuant to this Agreement, ensure that it makes available clear and sufficient information to Data Subjects as required by the Data Protection Legislation; and,

7.7.4. it shall take Protective Measures in relation to Personal Data, and in particular shall ensure that Personal Data transferred by the Member Organisation to the Force is hashed, compressed, encrypted at rest at 256bit AES and transmitted to the Force over Hypertext Transfer Protocol Secure (HTTPS).

7.8. The Parties acknowledge and declare that the sharing of Personal Data from the Member Organisation to the Force in the context of Police CyberAlarm involves a transfer of data from the Member Organisation as a Controller to the Force as a Controller.

7.9. The Parties acknowledge and agree that:

7.9.1. the Member Organisation shall be the Controller in respect of, and shall be solely responsible for, the collection, retention, and use by the Member Organisation of Personal Data and for the lawfulness of its disclosure of Member Organisation Data to the Force, as well as in connection with the Member Organisation's processing of any Personal Data contained within Police CyberAlarm Reports provided to the Member Organisation; and,

7.9.2. the Force shall be the Controller in respect of, and shall be solely responsible for, its processing of Police Data, including any data sharing by the Force.

7.10. Nothing in this Agreement is intended to, or shall be deemed to, establish any joint Controller arrangement between the Parties.

7.11. 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 Agreement 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.

7.12. The Parties each agree to promptly provide to the other such assistance as is reasonably required to enable the other Party to comply with its obligations under the Data Protection Legislation in relation to processing pursuant to this Agreement.

7.13. The Parties each agree to promptly notify the other in the event that, in respect of Personal Data processed in the context of this Agreement:

7.13.1. It receives any communication from a Supervisory Authority or any other regulatory authority;

7.13.2. It receives a Data Subject Request or any other request, complaint, communication, threatened claim or claim relating to either Party's obligations under the Data Protection Legislation; and/or,

7.13.3. It is obliged to rectify, erase or restrict personal data which has been disclosed to the other Party.

7.14. 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.

7.15. In each instance identified at clause 7.13 above, the Parties shall afford the other the opportunity to make written representations regarding the timing and content of any response, and shall consider such written representations in good faith prior to responding to the relevant Data /subject, Supervisory Authority, other regulatory authority or third party.

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

7.17. The Force, or such other person acting on behalf of the Force, shall undertake periodic reviews of the processing of Personal Data pursuant to this Agreement to ensure its ongoing compliance with the Data Protection Legislation and other Law.

8. Intellectual Property

8.1. The Member Organisation acknowledges and agrees that all Intellectual Property Rights in or relating to Police CyberAlarm, including in the logo, website, services, system, and any documentation relating to Police CyberAlarm, including Police CyberAlarm Reports, are and shall remain the property of the Force and/or its licensors.

8.2. All Intellectual Property Rights in respect of the Police Data shall be owned by and vest in the Force.

8.3. The Force hereby grants to the Member Organisation within the jurisdiction for the Term of this Agreement and subject to, and in accordance with, the terms of this Agreement, a non-exclusive licence to copy, publish, distribute, transmit and adapt the information contained within any Police CyberAlarm Report, subject to clause 8.2 above, solely for the Member Organisation's internal use and provided that the Member Organisation acknowledges the source of the information.

8.4. The Force grants the Member Organisation, or shall procure the direct grant to the Member Organisation of, a fully paid-up, worldwide, non-exclusive, royalty-free licence to copy, reproduce and to publish on the Member Organisation's own website and/or in its own marketing materials the Member Badge for the purpose of receiving and using the Membership Benefits solely during the Term of this Agreement and subject to, and in accordance with, the terms of this Agreement and the Branding Guidelines.

8.5. The Force warrants that the receipt, and use of the Member Badge by the Member Organisation in the manner permitted by this Agreement shall not infringe any rights of third parties to the extent that infringement results from copying.

8.6. Unless expressly stated otherwise, nothing in this Agreement shall constitute any representation or warranty that the exercise by the Member Organisation of rights granted under this Agreement will not infringe the rights of any person.

8.7. Subject to clauses 8.9 and 8.10, the Force shall indemnify the Member Organisation in full against any sums awarded by a court against the Member Organisation, and other claims, causes of action, and demands arising out of or in connection with any claim brought by a third party against the Member Organisation to enforce its Intellectual Property Rights to the extent that infringement results from copying arising out of or in connection with the authorised receipt or use of the Member Badge, save that the Force shall not be in breach of the warranty at clause 8.5 and the Member Organisation shall not be entitled to any indemnity to the extent that the infringement arises from any modification of the Member Badge.

8.8. The Member Organisation indemnifies the Force in full against any sums awarded by a court against the Force, and other claims, causes of action, and demands arising out of or in connection with any infringement of a third party's Intellectual Property Rights arising out of, or in connection with, the receipt or use of the Member Organisation Data.

8.9. The Parties shall immediately notify the other in writing giving full particulars if any of the following matters come to their attention:

8.9.1. any actual, suspected or threatened infringement of the Intellectual Property Rights;

8.9.2. any claim made or threatened that the Member Badge, or other material within the scope of the Intellectual Property Rights, infringe the rights of any third party; or

8.9.3. any other form of attack, charge or claim to which the Intellectual Property Rights may be subject.

8.10. In respect of any of the matters listed in clause 8.8 above:

8.10.1. the Force shall, at its absolute discretion, decide what action to take, if any;

8.10.2. the Force shall have exclusive control over, and conduct of, all claims, negotiations, and proceedings, provided that the Force considers and defends any IPRs claim diligently, using competent counsel and in such a way as not to bring the reputation of the Indemnified Party into unjustified disrepute;

8.10.3. the Member Organisation shall not make any admissions other than to the Force and shall provide the Force with all assistance that it may reasonably require in the conduct of any claims or proceedings, save that the Force may settle the claim (after giving prior written notice of the terms of settlement (to the extent legally possible) to the Member Organisation, but without obtaining the Member Organisation's consent) if the Force reasonably believes that failure to settle the Claim would be prejudicial to it in any material respect;

8.10.4. the Member Organisation shall give the Force and its professional advisers access at reasonable times (on reasonable prior notice) to its premises and its officers, directors, employees, agents, representatives or advisers, and to any relevant assets, accounts, documents and records within its power or control, so as to enable the Force and its professional advisers to examine them and to take copies (at the Member Organisation's expense) for the purpose of assessing the claim;

8.10.5. the Force shall bear the cost of any proceedings and shall be entitled to retain all sums recovered in any action for its own account; and,

8.10.6. subject to the Member Organisation providing security to the Force to the Force's reasonable satisfaction against any claim, liability, costs, expenses, damages or losses that may be incurred, and subject always to clause 8.10.1, the Force may agree to take such action as the Member Organisation may reasonably request to avoid, dispute, compromise or defend the Claim.

8.11. The provisions of sections 101 and 101A of the Copyright, Designs and Patents Act 1988 (or equivalent legislation in any jurisdiction) are expressly excluded.

8.12. Nothing in this clause 8 shall restrict or limit the Parties' general obligation at law to mitigate a loss it may suffer or incur as a result of an event that may give rise to a claim under the indemnity at clause 8.7 or clause 8.8.

8.13. The Member Organisation shall:

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

8.13.2. comply with all regulations and practices in force or use in the Territory to safeguard the Intellectual Property Rights of the Force and/or its licensors.

8.14. The Member Organisation shall not do or omit to do anything to diminish the Intellectual Property Rights of the Force or its licensors, nor assist any other person to do so, whether directly or indirectly.

8.15. The Member Organisation acknowledges and agrees that the exercise of the licence granted to the Member Organisation under this Agreement is subject to all applicable laws, enactments, regulations and other similar instruments in the Territory, and the Member Organisation understands and agrees that it shall at all times be solely liable and responsible for such due observance and performance.

9. Assignment & other dealings

9.1. The Member Organisation shall not assign, transfer, mortgage, charge, sub-license, subcontract, delegate, declare a trust over or deal in any other manner with any or all of its rights and obligations under this Agreement without the prior written consent of the Force.

9.2. The Force may at any time assign, transfer, mortgage, charge or deal in any other manner with any or all of its rights and / or obligations under this cause of the Contract, provided that the Centre gives written notice to the Member.

9.3. Notwithstanding clause 10.1 below, the Force when assigning any or all of its rights under this clause of the Agreement may disclose to a proposed assignee any information in its possession that relates to this agreement or its subject matter, the negotiations relating to it and the Member Organisation which it is reasonably necessary to disclose for the purposes of the proposed assignment.

9.4. The Force may subcontract or delegate in any manner any or all of its obligations under this agreement to any third party.

9.5. The Member Organisation shall, at the Force's request, execute any agreements or other instruments (including any supplement or amendment to this agreement) which may be required in order to give effect to or perfect any assignment, transfer, mortgage, charge or other dealing referred to in clause 9.2 above.

10. Confidentiality

10.1. Each party undertakes that it shall not at any time use or disclose to any person the other Party's Confidential Information, except as permitted by this clause 10.

10.2. Each party may disclose the other Party's Confidential Information:

10.2.1. to its employees, officers, representatives, contractors, subcontractors or advisers who need to know such information for the purposes of carrying out the party's obligations under the Agreement. Each party shall ensure that its employees, officers, representatives, contractors, subcontractors or advisers to whom it discloses the other party's Confidential Information are made aware of its confidential nature and comply with this clause 10; and

10.2.2. as may be required by law, a court of competent jurisdiction or any law enforcement agency, governmental or regulatory authority, in which case the Discloser shall immediately notify the other Party in writing of any such requirement for disclosure of the Confidential Information in order to allow the Discloser to make representations to the person or body imposing the requirement.

10.3. The restriction contained in clause 10.1 above shall cease to apply to any Confidential Information which may come into the public domain otherwise than through unauthorised disclosure by the Parties to this Agreement, their officers, employees, servants or agents.

11. Limitation of Liability

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

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

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

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

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

11.2. Subject to clause 11.1 above, neither Party shall in any circumstances be liable whether in contract, tort (including for negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for:

11.2.1. Any loss or damage to (whether direct or indirect) of revenue, profits, sales or business, business opportunities, revenue, turnover, reputation or goodwill;

11.2.2. Loss (whether direct or indirect) of anticipated savings or wasted expenditure (including management time);

11.2.3. Any other consequential loss;

11.2.4. Any loss or liability (whether direct or indirect) under or in relation to any other contract.

11.3. Subject to clauses 8 (Intellectual Property) and 11.1 above, the Force shall not be liable in contract, tort (including negligence), breach of statutory duty or otherwise for any loss or damage of whatsoever kind and howsoever arising in connection with the installation, operation or removal of Police CyberAlarm, including the loss of use or corruption of software, data or information, or the provision of, failure to provide, or reliance on Police CyberAlarm Reports provided to the Member Organisation as a consequence of the use of Police CyberAlarm.

11.4. Neither Party may benefit from the limitations and exclusions set out in this clause 11 in respect of any liability arising from its deliberate default. Nor may either Party benefit from any indemnity in this Agreement to the extent that a claim under it results from the Indemnified Party's negligence or wilful misconduct.

11.5. Subject to clauses 11.1 – 11.4 above and clause 11.6 below, the Parties' respective total aggregate liability in connection with this Agreement (whether in contract, tort (including negligence), breach of statutory duty or howsoever arising) shall be limited to a sum of £5,000.

11.6. The caps on the parties' liabilities shall not be reduced by:

11.6.1. payment of an uncapped liability;

11.6.2. amounts awarded or agreed to be paid under clause 8 (Intellectual Property); and

11.6.3. amounts awarded by a court or arbitrator, using their procedural or statutory powers in respect of costs of proceedings or interest for late payment.

11.7. Unless the Member Organisation notifies the Force that it intends to make a claim in respect of an event within the Notice Period, the Force shall have no liability for that event. The Notice Period for an event shall start on the day on which the Member Organisaton became, or ought reasonably to have become, aware of the event having occurred and shall expire three months from that date. The notice must be in writing, be sent by recorded

delivery to the Force Headquarters, and must identify the event and the grounds for the claim in reasonable detail.

The Parties acknowledge and agree that the limitations contained in this clause 11 are commercially reasonable in the light of the nature of the Agreement, the identity of the Parties and all the relevant circumstances relating to provision of Police CyberAlarm.

12. Disputes

12.1. In the event of any dispute or difference between the Parties arising out of this Agreement, the representatives of the Parties to the dispute or difference shall, within 20 days of receipt of a written request from any party to the dispute, meet in an effort to resolve the dispute or difference in good faith.

12.2. The Parties will, with the help of The Centre for Effective Dispute Resolution, seek to resolve disputes between them by alternative dispute resolution. If the Parties fail to agree within 56 days of the initiation of the alternative dispute resolution procedure, then the Parties shall be at liberty to commence litigation.

13. Miscellaneous

13.1. Where the Force receives a request for information under the provisions of the Freedom of Information Act 2000 in respect of Data provided by or relating to a specific Member Organisation, the Force may contact the Member Organisation to ascertain whether the Member Organisation wishes to claim any exemption and to obtain information to support any such claim. The Force shall be entitled to determine, in its sole discretion, the response to the request.

13.2. This Agreement, and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation, shall be governed by, and construed in accordance with the law of England and Wales.

13.3. Each Party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with the Agreement or its subject matter or formation.

13.4. This Agreement constitutes the entire agreement between the Parties as regards the subject matter hereof and supersedes all prior oral or written agreements regarding such subject matter.

13.5. If any provision of this Agreement is held by a Court of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect the remaining provisions of this Agreement, which shall remain in full force and effect.

13.6. Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between the Parties or authorise any Party to make or enter into any commitments for or on behalf of any other Party.