CYBERALARM

DATA SHARING AGREEMENT

THIS CONTRACT is made on the date that the Member Organisation provides all required information and submits its electronic signature via the website: [INSERT URL]

BETWEEN

1. The Parties

1.1 The company or entity sharing data in respect of which it is a data controller to the relevant Law Enforcement Entity, (herein after called the "Member Organisation" of the one part and The Chief Constable of the referring force (herein after called the "Law Enforcement Entity"), of the other part.

2. **Background**

2.1 This Contract sets out the terms and conditions under which personal data held by the specified Member Organisation's Controller will be disclosed to the specified Law Enforcement Controller. This Contract is entered into with the purpose of ensuring compliance with the applicable "Data Protection Legislation". Any processing of personal data by the Parties pursuant to this Contract must comply with the provisions of this legislation.

3. Purpose

3.1 The purpose of the processing is to detect and disrupt cybercrime, reduce the incidence of cybercrime and to protect the public from harm. The Parties consider that the processing pursuant to the data sharing initiative under this Contract is necessary for this purpose. This will be enabled by the Law Enforcement Entity being given access to a Member Organisation's internet facing firewall and network to, variously and as agreed to by the Member Organisation when submitting its electronic signature:

(a) vulnerability scan their public facing IP addresses on either a one off or repeated basis so that a vulnerability assessment can be undertaken and report provided to the Member Organisation to enable them to mitigate any vulnerability identified. It is the Member Organisations responsibility to mitigate the identified vulnerabilities. The Law Enforcement Entity will retain a copy of the report so when appropriate they can provide face to face crime prevention advice. The Law Enforcement Entity will also use the aggregated data to identify and assess the Cybercrime risk and threat.

(b) vulnerability scan their websites and Web Applications on either a one off or repeated basis so that a vulnerability assessment can be undertaken and report provided to the Member Organisation to enable them to mitigate any vulnerability identified. It is the Member Organisation's responsibility to mitigate the identified vulnerabilities. The Law Enforcement Entity will retain a copy of the report so when appropriate they can provide face to face crime prevention advice. The Law Enforcement Entity will also use the aggregated data to identify and assess the Cybercrime risk and threat.

(c) collect on an ongoing basis the Firewall Logs including the Packet Header Information and the IP address of the originating sender of Suspicious Firewall Activity data. The Law Enforcement Entity will retain and analyse this Suspicious Firewall Activity data, and process the data for other law enforcement purposes.

The above will be facilitated by the Member Organisation utilising any one or more of the three Pervade Police Cyber Alarm tools listed below, (herein after called the Purpose.)

3.2 The following Pervade Police CyberAlarm (PCA) tools will be used for the completion of the 'Purpose':

3.2.1 Pervade Police Cyber Alarm - External Network Vulnerability Scanner - To conduct the PCA Vulnerability Scan on the Member Organisations external network points the system utilises OpenVAS (an open source vulnerability scanner), which is deployed against the Volunteer Organisation's identified public IP addresses. (These are recorded during signup). The scanner is deployed from the PCA central server which then identifies which vulnerabilities the Member Organisation is open to. The Member Organisation will then receive a report identifying any known external vulnerabilities to its network. It will be the Volunteer Organisation's responsibility to action any highlighted vulnerability. The Law Enforcement Entity will retain a copy of the report so when appropriate they can provide direct crime prevention advice. The Law Enforcement Entity will also use the aggregated data to identify and assess the cybercrime risk and threat and for other law enforcement purposes.

3.2.2 Pervade Police Cyber Alarm – Website & Web App Vulnerability Scanner – To conduct the PCA Vulnerability Scan on the Member Organisations websites and web applications the system utilises Nikto (recorded during sign up) allowing the system to provide vulnerability scanning of websites and web applications. This includes testing for SQL injection, Cross-Site Scripting (XSS) and Layer 7 denial of service attacks amongst other attacks. The Member Organisation will then receive a report identifying any known external vulnerabilities to their websites. It will be the Member Organisation's responsibility to action any highlighted vulnerability. The Law Enforcement Entity will retain a copy of the report so when appropriate they can provide direct crime prevention advice. The Law Enforcement will also use the aggregated data to identify and assess the Cybercrime risk and threat and for other law enforcement purposes.

3.2.3 Pervade Police Cyber Alarm - Network Traffic Analyser – This tool is used to collect the Firewall Logs containing Packet Header Information including the IP address of the originating sender of Suspicious Firewall Activity as a result of the Member Organisation installing a software node. The Member Organisation will share this data with the Law Enforcement Entity will process this Suspicious Firewall Activity data for law enforcement purposes, which may include:

a) to identify when a Member Organisation is under attack in and inform the Law Enforcement Entity of this attack to enable the gathering of intelligence as to the scale and nature of the threat and, at the sole discretion of the Law Enforcement Entity and consistent with the scale and nature of the incident and the Law Enforcement Entity's resources, priorities and operational judgement, to take any action it may deem necessary or appropriate which may include notifying the Member Organisation of the attack"; and
b) provide an automated Cyber Security Report to the Member Organisation detailing the type and frequency of attacks to enable the Member Organisation take such steps as they deem necessary and appropriate at their own expense toenable the Member Organisation to better protect themselves.

c) to enable the analysis of the aggregated crowd sourced log files (the combination of multiple organisations either at a Force, Regional or National level) to identify subject(s) involved in Cybercrime and to use this data to enrich the intelligence picture within the UK on the types and frequency of Cyber-attacks against the UK infrastructure.

3.4 The Member Organisation warrants that the Purpose is consistent with the original purpose of the data collection.

4. Definitions

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

4.2 In this Contract, 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.

4.3 **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.

4.4 **Special Categories of Personal Data** has the same meaning as in Article 9 of the GDPR.

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

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

4.7 **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.

4.8 **Data Subject Access 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 their personal data.

4.9 **Police Data** means any Data including Personal Data, Special Categories of Personal Data and criminal conviction and offence data, to be provided to, or collected by, the Law Enforcement Entity and processed by them as identified in this Contract.

4.10 **Member Organisation** means a business that agrees to undertake vulnerability scanning and/or installs on their internet facing firewall device the Pervade Police Cyber Alarm software node.

4.11 The **Designated 'Member Organisation' Manager** means a person who has the day to day responsibility for the management of the Purpose on behalf of the Member Organisation or other such person as shall be notified to the Law Enforcement Entity from time to time.

4.12 The **Police Project Manager** means a person who has the day to day management on behalf of the Law Enforcement Entity, or such other person as shall be notified to the Member Organisation from time to time.

4.13 **Government Security Classification** means a scheme for the classification of information.

4.14 **Contract** means this Data Sharing Contract together with its schedules and all other documents attached to or referred to as forming part of this Contract, including information submitted by the Member Organisation when submitting its electronic signature.

4.15 **Data Protection Impact Assessment** means an assessment by the relevant Controller of the impact of the envisaged processing on the protection of personal data.

4.16 **Services** means the processing activities and services to be undertaken by the Law Enforcement Entity on behalf of the Volunteer Organisation, as identified.

4.17 **Protective Measures** means 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 such measures adopted.

4.18 **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 Processor is bound to comply.

4.19 **Confidential Information** means all Police Data and any other information relating to the Member Organisation's customers and prospective customers, current or projected financial or trading situations, business plans, business strategies, developments and all other information relating to the Volunteer Organisation's business affairs including any trade secrets, know-how and any information of a confidential nature imparted by the Member Organisation to the Law Enforcement Entity during the term of this Contract or coming into existence as a result of the Law Enforcement Entity's obligations, whether existing in hard copy form or otherwise, and whether disclosed orally or in writing.

4.20 **Content** means the files, data, text and other materials that are transferred, stored, shared or hosted on or through the Services and Software by the Law Enforcement Entity, Users and Recipients, including any Personal Data in it. It does not include CRM Information or System Data.

4.21 **Suspicious Firewall Activity data** any activity highlighted by the Pervade Police Cyber Alarm - Network Traffic Analyser system as potentially being an attack or part of an attack.

Interpretation

4.22 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;

4.23 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.

4.24 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.

5. Information provision

5.1 Details of the Member Organisation Data to be provided to or collected by the Law Enforcement Entity are set out at clause 3 above. To enable this the Member Organisation will install the relevant software and shall provide the following details to the Law Enforcement Entity when it submits its electronic signature, together with any other information requested by the Law Enforcement Entity as part of submission:

(a) Name of its nominated point of contact;

(b) Address of its headquarters and/or server storage facility;

(c) Email address of the Data Protection Officer or other individual with responsibility for data protection compliance at the Member Organisation; and

(d) IP addresses/public network address range.

5.2 It is recognised that the Purpose requires access to Member Organisation Data as at clause 3 above and the Parties agree that any Personal Data shared pursuant to this Contract is relevant and not excessive to the Purpose.

5.3 The Member Organisation can either sign up to only the Network Traffic Analyser or one or both of the Vulnerability Scanners. In the case of the Vulnerability Scanner components this could be carried out as an automated one-off check or the Voluntary Organisation can set this to be done regularly, with a maximum frequency of monthly. The Network Traffic Analyser would collect data continuously. The Member Organisation can opt out at any time and the Services will cease.

5.4 The Police Data will be automatically encrypted to 256-bit AES by the Police CyberAlarm System before being transmitted or collected from the Member Organisation.

5.5 Where legitimate data are inadvertently collected within the Suspicious Firewall Activity these will be destroyed beyond being retrievable by the Law Enforcement Entity within a reasonable period of this being identified.

6. Use, Disclosure and Publication

6.1 The Member Organisation Data be processed in accordance with the Purpose and shall not otherwise be processed in a manner that is incompatible with the Purpose. This section does not apply to the Police copy of the Vulnerability Reports and the 'suspicious activity data'.

6.2 Unless in accordance with the "Purpose", the identity of the Member Organisation as being a recipient of the Services will not be disclosed by the Law Enforcement Entity to any third party without the written authority of the Member Organisation.

6.3 All rights in respect of the data collected or created by the Law Enforcement Entity in connection with this Contract, and the ownership and title to all documents and physical materials created in connection with this Contract, shall be owned by and vest in the Law Enforcement Entity. These shall be classified as Police Data.

6.4 The Law Enforcement Entity hereby grants to the Member Organisation within the jurisdiction for the Term of this Contact and subject to, and in accordance with, the terms of this Contract, a non-exclusive licence to copy, publish, distribute, transmit and adapt the information contained within any document subject to clause 6.3 above solely for the Member Organisation's internal use provided that the Member Organisation acknowledges the source of the information.

7. **Data Protection and Human Rights**

7.1 The use and disclosure of any Personal Data shall be in accordance with the obligations imposed upon the Parties to this Contract by the Data Protection Legislation and the Human Rights Act 1998. All relevant codes of practice or data protection operating rules adopted by the Parties will also reflect the data protection practices of each of the Parties to this Contract.

7.2 The Parties agree and declare that the information accessed pursuant to this Contract will be used and processed with regard to the rights and freedoms enshrined within the European Convention on Human Rights. Further, the Parties agree and declare that the provision of information is proportionate, having regard to the Purpose and the steps taken in respect of maintaining a high degree of security and confidentiality.

7.3 The Parties undertake to comply with the provisions of the Data Protection Legislation at all times during the Term of this agreement and in particular to notify as required any particulars as may be appropriate to the Information Commissioner. Each Party has 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 cover data sharing pursuant to this Contract, unless an exemption applies.

7.4 In particular, the Member Organisation warrants that it has legitimate grounds under the Data Protection Legislation to process the Personal Data as envisaged by this Contract and the right to share the Suspicious Activity Firewall data with the Law Enforcement Entity for the Purpose.

7.5 The Member Organisation shall, in respect of Personal Data to be shared pursuant to this Contract, ensure that it provides clear and sufficient information to Data Subjects as required by the Data Protection Legislation. In order to comply with its obligations under the Data Protection Legislation, the Member Organisation shall ensure that it provides appropriate information to Data Subjects including in relation to the sharing of information pursuant to this Contract. In order to assist the Member Organisation in complying with its obligations in this regard, and without accepting liability for the accuracy or adequacy of the information contained therein, the Law Enforcement Entity provides the following information which the Member Organisation may wish to have regard to in providing transparency information to Data Subjects:

As part of our cyber security monitoring we share the Metadata of all traffic deemed to be suspicious with the Police for law enforcement purposes. The Data Controller with whom your data is shared is [IDENTIFY RELEVANT FORCE].
This Metadata relating to the network traffic does not contain any information relating to the contents of the traffic, merely the destination, originating IP address and the 'packet header' of the request.
In order to comply with a subject access request in relation to this processing and to be able to advise you as to whether your data has been shared and with whom, we will need you to share with us the IP address used to access our network and the date time including time zone of the access. If you have a dynamically allocated IP address, as is likely for home users, we would need to know the IP address(es) allocated to you for the period you are enquiring about. This information may be obtained from your Internet Service Provider.

7.6 The Law Enforcement Entity shall not retain or process Personal Data pursuant to this Contract for longer than is necessary for the Purpose.

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

7.8 The Law Enforcement Entity and the person representing the Member Organisation as notified when the Member Organisation submits its electronic signature shall notify the

other Party within 72 hours should either Party, in respect of the Personal Data processed pursuant to this Contract:

(a) receive a Data Subject Access Request (or purported Data Subject Access Request) before responding to the Data Subject;

(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 a Supervisory Authority or any other regulatory authority in connection with Personal Data processed under this Contract;

(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;

(f) becomes aware of a Data Loss Event; and,

in each case the Parties shall consider any written representations provided by the other Party in good faith prior to responding to the relevant data subject, Supervisory Authority, other regulatory authority or third party.

7.9 The Parties' respective obligations to notify the other under the preceding clause 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 a Data Loss Event or any communication from a Supervisory Authority or other regulatory authority or third party.

7.10 The Parties shall be responsible for maintaining a record of any request or communication detailed at clause 7.8 above.

7.11 Where the Law Enforcement Entity receives a request for information under the provisions of the Freedom of Information Act 2000 in respect of information provided by or relating to the Member Organisation, the Law Enforcement Entity will contact the person nominated below to ascertain whether the Member Organisation wishes to claim any exemption including the determination of whether or not the Law Enforcement Entity wishes to issue a response neither to confirm nor deny that information is held.

7.12 The Law Enforcement Entity's Data Protection Officer is to assume responsibility for Data Protection legislation compliance, notification, security, confidentiality, audit and co-ordination of Data Subject rights on behalf of the Law Enforcement Entity. The Member's Organisation's Data Protection Officer or other individual with responsibility for data protection compliance on behalf of the Member Organisation as notified by the Member Organisation when submitting its electronic signature assume responsibility for Data Protection legislation compliance, notification, security, confidentiality, audit and co-ordination of Data Subject rights on behalf of the Member Organisation.

7.13 The Parties agree to take account of any guidance issued by the Supervisory Authority relevant to their obligations under this Contract. The Parties may agree or, on not less than 30 Working Days' notice to the other Party, amend this Contract to ensure that it complies with any guidance issued by the Supervisory Authority.

7.14 Respect for the privacy of individuals will be afforded at all stages of the Purpose.

8 Confidentiality

8.1 Except as specified in clause 7.2 below, the Parties shall not use or divulge or communicate to any person (other than those whose province it is to know the same for the Purpose) any Confidential Information.

8.2 Clause 8.1 above shall not apply where disclosure of the Confidential Information is ordered by a Court of competent jurisdiction, or subject to any exemption under the Data Protection Act 2018, where disclosure is required by a law enforcement agency or regulatory body or authority, or is required for the purposes of legal proceedings, in which case the Processor shall immediately notify the Controller in writing of any such requirement for disclosure of the Police Data in order to allow the Controller to make representations to the person or body making the requirement.

8.3 The restrictions contained in clauses 8.1 and 8.2 shall cease to apply to any Data which may come into the public domain otherwise than through unauthorised disclosure by the Parties to the Contract.

8.4 For the avoidance of doubt, the obligations of confidentiality imposed on the Parties by this Contract shall continue in full force and effect after the expiry or termination of this Contract.

9 Retention, Review and Deletion

9.1 All the Data (as at clauses 3 and 5.1 above) will be subject to the normal policies and procedures of the Parties in relation to the retention, review and disposal.

9.2 Electronic copies of the data shall be securely destroyed by either physical destruction of the storage media or secure deletion using an approved CESG data cleansing product.

10 Security

10.1 The Parties recognise their obligations relating to the security of Data in under their control under the Data Protection Legislation, and the relevant standards and guidance (including ISO 27001 and the Information Community Security Policy for policing). The Parties shall continue to comply with those obligations, having regard to relevant standards and guidance, as detailed below during the term of this Contract.

10.2 The Parties shall in assessing the appropriate level of security take particular account of the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

11 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, 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 (whether direct or indirect) of profits, 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); or

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

11.3 Subject to clauses 11.1 and 11.2 above, the Parties' total aggregate liability in connection with this Contract, which shall be apply throughout the duration of this Contract (whether in contract, tort (including negligence), breach of statutory duty or howsoever arising) shall be limited to a sum of £100,000.

12 Disputes

12.1 In the event of any dispute or difference arising between the Parties out of this Contract, the persons appointed pursuant to clause 7.12 of this Contract and representing the Parties to the dispute or difference shall within 20 days of receipt of a written request from any party to the dispute addressed to one of the individuals described at section 6.11 meet in an effort to resolve the dispute or difference in good faith.

12.2 This Contract is subject to English Law and the jurisdiction of the English Courts. The Parties will, with the help of a Centre for 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 Term Termination and Variation

13.1 This Contract shall commence on installation of the Pervade Cyber Alarm software and shall operate until completion of the Purpose or any party wishes to exit from this Contract, whichever is the sooner (the 'Term').

13.2 In the event that the Member Organisation wishes to exit from this Contract, that Party shall uninstall the relevant software from their system.

13.3 The Law Enforcement Entity shall be entitled to exit from this Contract at any time and shall do so by ceasing to collect further Personal Data pursuant to the Contract.

14 Miscellaneous

14.1 This Contract 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.

14.2 If any provision of this Contract 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 Contract, which shall remain in full force and effect.

14.3 The validity, construction and interpretation of the Contract and any determination of the performance which it requires shall be governed by the Laws of England and the Parties hereby submit to the exclusive jurisdiction of the English Courts.

14.4 Nothing in this Contract 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.

.....