EU DATA PROCESSING ADDENDUM

(Last Updated: 02/01/2021)

This Data Processing Addendum ("**Addendum**") forms part of the agreement between Arctic Wolf Networks, Inc. and Customer for the purchase of products and/or solutions identified in the agreement (collectively, the "**Solutions**") from Arctic Wolf (the "**Agreement**"). Each of Customer and Arctic Wolf may be referred to herein as a "**party**" and together the "**parties**".

How this Addendum applies

Data protection laws worldwide, including the GDPR (as defined below), place certain obligations upon a data controller to ensure that any data processor it engages provides sufficient guarantees to ensure that the processing of the personal data carried out on its behalf is secure.

This Addendum exists to ensure that there are sufficient security guarantees in place and that the processing conducted by Arctic Wolf on behalf of Customer complies with obligations equivalent to those in the GDPR.

How to accept this Addendum

This Addendum consists of two parts: the main terms, and Appendix 1 (Standard Contractual Clauses).

To accept this Addendum:

1. **Complete the Customer information in the signature boxes and sign and date page 5;**
2. **Sign page 11 (Exhibit B - Standard Contractual Clauses);**
3. **Sign page 12 (Appendix 1 1 to Standard Contractual Clauses); and**
4. **Send the completed and signed Addendum to Arctic Wolf at legal@arcticwolf.com.**

The Customer entity signing this Addendum must be the same as the Customer entity party to the Agreement.

If the entity signing this Addendum is not a party to the Agreement directly with Arctic Wolf, this Addendum is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this Addendum.

This Addendum has been pre-signed on behalf of Arctic Wolf. Any changes to this Addendum, other than completion of information and execution in the signature boxes on the pages referenced above, renders Arctic Wolf's signature to this Addendum null and void.

The date of this Addendum shall be the later of the date set forth on page 5 in Customer's signature box and the date when a signed copy of this Addendum is received by Arctic Wolf as described above.

EU Data Processing Addendum

1. Definitions. Any capitalized terms not otherwise defined in this Addendum shall have the meaning set forth in the Solutions Agreement (also referred to as the Master Solutions Agreement). In this Addendum, the following terms shall have the meaning set forth as follows:

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists, or (iv) regardless of ownership, any company or other entity, whether or not with legal personality, which directly or indirectly, is under joint control with a party.

1.2 "Anonymous Data" means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person.

1.3 "Authorized Employee" means an employee of Processor who has a need to know or otherwise access Personal Data to enable Processor to perform their obligations under this Addendum or the Agreement.

1.4 "Authorized Sub-Processor" means a third-party who has a need to know or otherwise access Personal Data to enable Processor to perform its obligations under this Addendum or the Agreement, and who is either (1) listed at https://arcticwolf.com/terms/sub-processors/ or (2) authorized by Controller to do so under Section 4.2 of this Addendum.

1.5 "Customer" means the customer entity that is party to the Solutions Agreement.

1.6 "Data Subject" means an identified or identifiable person to whom Personal Data relates that is located in the European Economic Area or the United Kingdom ("UK").

1.7 "Data Protection Laws" means (1) the Regulation (EU) 2016/679 of the European Parliament, the General Data Protection Regulation ("GDPR") as implemented and applied by Member States and (2) the UK GDPR.

1.8 "Instruction" means a direction, either in writing, in textual form (e.g. by e-mail) or by using a software or online tool, issued by Controller to Processor and directing Processor to Process Personal Data.

1.9 "Personal Data" means any information relating to Data Subject which is subject to Data Protection Laws (defined below) and which Processor Processes on behalf of Controller other than Anonymous Data.

1.10 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

1.11 "Process" or "Processing" means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.12 "Restricted Transfer" shall have the meaning set forth in the GDPR.

1.13 "Solutions" shall have the meaning set forth in the Agreement.

1.14 "Standard Contractual Clauses" means an agreement that may be entered into by and between Controller and Processor pursuant to the European Commission's decision (C(2010)593) of February 5, 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection (or any updated version thereof). The Standard Contractual Clauses are attached hereto as part of Exhibit B.

1.15 "Supervisory Authority" means an independent public authority which is established by a member state of the European Union, Iceland, Liechtenstein, Norway, or the United Kingdom.

1.16 "UK GDPR" means the GDPR as amended and incorporated into UK law pursuant to the UK Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

2. Processing of Data

2.1 Roles of the Parties. The parties and acknowledge and agree that, with regard to the Processing of Company Personal Data pursuant to the Agreement, Customer is the "Controller" and Arctic Wolf is the "Processor," as those terms are defined under the Data Protection Laws. Processor may engage Authorized Sub-Processors as set forth herein.

2.2 Controller's Processing of Personal Data. Controller shall, in its use of the Solutions, at all times Process Personal Data, and provide instructions for the Processing of Personal Data, in compliance with the Data Protection Laws. Controller shall ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Personal Data, and that the Processing of Personal Data in accordance with Controller's instructions will not cause Processor to be in breach of the Data

Protection Laws. Controller is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Processor by or on behalf of Controller, (ii) the means by which Controller acquired any such Personal Data, and (iii) the instructions Controller provides to Processor regarding the Processing of such Personal Data. Controller is likewise responsible for ensuring that its transfer of Personal Data to Processor will comply with Data Protection Laws. Controller shall not provide or make available to Processor any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Solutions, and shall indemnify Processor from all claims and losses in connection therewith.

2.3 Processor's Processing of Personal Data. Processor shall comply with its processor obligations under the Data Protection Laws. Processor, however, is not responsible for compliance with any Data Protection Laws or other laws applicable to Controller or Controller's industry that are not otherwise applicable to Processor. Processor shall only Process the Personal Data as necessary to perform its obligations under the Agreement (including Exhibit A) and to provide the Solutions. Processor shall not Process Personal Data in a manner inconsistent with Controller's documented instructions, including the terms and conditions set forth in this Addendum.

2.4 Details of the Processing. The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this Addendum.

2.5 Deletion or Return of Personal Data. Following completion of the Solutions, at Controller's request, Processor shall return or delete the Personal Data (including Personal Data in the possession of Authorized Sub-Processors), unless further storage of Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Processor shall take measures to block such Personal Data from any further Processing (except to the extent necessary for its continued hosting or Processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Controller and Processor have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 14(1) of the Standard Contractual Clauses shall be provided by Processor to Controller only upon Controller's request.

3. Authorized Employees. Processor shall ensure that its Authorized Employees are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed confidentiality agreements that survive the termination of their engagement with Processor.

4. Authorized Sub-Processors

4.1 Controller agrees that Processor has general authority to engage third parties, partners, agents, or service providers, including its Affiliates, to Process Personal Data on Controller's behalf in order to provide the solutions contemplated in the Agreement agreed to by Controller ("Authorized Subprocessors"). Processor shall not engage a subprocessor to carry out specific Processing activities which fall outside the general authority granted above without Controller's prior specific written authorization and, where such subprocess is so engaged, Processor shall ensure that the same obligations set out in this Addendum shall be imposed on that subprocessor.

4.2 A list of Processor's current Authorized Sub-Processors (the "List") is available to Controller at https://arcticwolf.com/terms/sub-processors/, which may be updated by Processor from time to time. Controller agrees to subscribe to receive notifications from the List of new Authorized Sub-Processors. At least ten (10) days before enabling any third party other than current Authorized Sub-Processors to access or participate in the Processing of Personal Data, Processor will add such third party to the List. Controller may reasonably object to the addition of any such third parties to the List by informing Processor in writing within ten (10) days of receipt of the aforementioned notice by Controller.

4.3 If Controller reasonably objects to an engagement in accordance with Section 4.2, and Processor cannot provide a commercially reasonable alternative within a reasonable period of time, Processor may terminate the Agreement. Termination shall not relieve Controller of any fees owed to Processor under the Agreement. If Controller does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Processor, that third party will be deemed an Authorized Sub-Processor for the purposes of this Addendum.

4.4 Processor will enter into a written agreement with each Authorized Sub-Processor that imposes obligations to protect Personal Data that are comparable to those imposed on Processor under this Addendum. Processor will remain liable to Controller for the non-performance of the Authorized Sub-Processor's data protection obligations under such agreement.

4.5 If Controller and Processor have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute Controller's prior written consent to the subcontracting by Processor of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Processor to Controller pursuant to Clause 5(j) of the Standard Contractual Clauses may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Processor beforehand, and that such copies will be provided by the Processor only upon request by Controller.

5. Security of Personal Data. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data.

6. Transfers of Personal Data

The parties agree that Personal Data processed under this Addendum may be transferred outside the EEA, Switzerland, or the UK as necessary to provide the Solutions. To the extent Processor initiates a Restricted Transfer, Processor will ensure that the transfer is subject to appropriate safeguards in accordance with Data Protection Laws. Mechanisms used for Restricted Transfers may include (without limitation) use of the Standard Contractual Clauses or (if appropriate) derogations available under Article 49 of the GDPR. As applicable, Controller (as "data exporter") and Processor (as "data importer") agree to complete and execute into the Standard Contractual Clauses (attached as Exhibit B) in connection with any Restricted Transfers initiated by Controller.

7. Rights of Data Subjects

7.1 Processor shall, to the extent permitted by law, notify Controller upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of Processing, objection to Processing, and/or objection to being subject to automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Processor receives a Data Subject Request in relation to Controller's data, Processor will advise the Data Subject to submit their request to Controller and Controller will be responsible for responding to such request, including, where necessary, by using the functionality of the Solutions. Controller is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of Processing, or withdrawal of consent to Processing of any Personal Data are communicated to Processor, and for ensuring that a record of consent to Processing is maintained with respect to each Data Subject.

7.2 Processor shall, at the request of the Controller, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Controller in complying with Controller's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Controller is itself unable to respond without Processor's assistance and (ii) Processor is able to do so in accordance with all applicable laws, rules, and regulations. Controller shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Processor.

8. Actions and Access Requests

8.1 Where Controller is obligated by Data Protection Laws to carry out a data protection impact assessment ("DPIA") relating to Controller's use of the Solutions, Processor shall provide reasonable cooperation and assistance to Controller for the DPIA to allow Controller to comply with its obligations under the Data Protection Laws. Controller shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Processor and Processor shall be entitled to involve Controller at Processor's then-current rates for any time expended in assisting with the DPIA.

8.2 Processor shall provide Controller with reasonable assistance to Controller in cooperation or prior consultation with any Supervisory Authority as may be required by Data Protection Laws. Controller shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Processor and Processor shall be entitled to involve Controller at Processor's then-current rates for any time expended in providing such assistance.

8.3 Where required by Data Protection Laws, Processors will assist Controller in demonstrating compliance with this Addendum by making available at the request of Controller, following reasonable notice to Processor, information reasonably necessary to demonstrate such compliance. Controller shall have the right to review, audit and copy such records at Processor's offices during regular business hours.

8.4 Upon Controller's request, Processor shall, no more than once per calendar year, either (i) make available for Controller's review copies of certifications or reports demonstrating Processor's compliance with prevailing data security standards applicable to the Processing of Controller's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Controller or its authorized representative, upon reasonable notice and at a mutually agreeable date and time, to conduct an audit or inspection of Processor's data security infrastructure and procedures that is sufficient to demonstrate Processor's compliance with its obligations under this Addendum, provided that Controller shall provide a minimum of thirty (30) days' prior notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Processor's business. Controller shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Processor for any time expended for on-site audits. If Controller and Processor have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 5(f) and Clause 13(2) of the Standard Contractual Clauses shall be carried out in accordance with this Section 8.4.

8.5 Processor shall within forty-eight (48) hours notify Controller if an instruction, in the Processor's opinion, infringes the Data Protection Laws or Supervisory Authority.

9. Personal Data Breach

9.1 In the event of a Personal Data Breach of Controller's Personal Data Processed by Processor or its Authorized Sub-Processors, Processor shall inform Controller of the Personal Data Breach without undue delay after having become aware of such Personal Data Breach. Further, Processor shall take all steps it deems necessary and reasonable (in its sole discretion) to investigate and remediate the Personal Data Breach, to the extent that remediation is within Processor's reasonable control.

9.2 In the event of a Personal Data Breach, Processor shall provide Controller with reasonable cooperation and assistance necessary for Controller to comply with its obligations under the Data Protection Laws relating to the Personal Data Breach, including with respect to any notification to Supervisory Authorities or Data Subjects affected by such Personal Data Breach. In providing such cooperation, Processor shall not be responsible for the failure of any notice to comply with Data Protection Laws or other damages that result from remedial actions to the extent such actions were requested or directed by Controller.

9.3 The obligations described in Sections 9.1 and 9.2 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Controller. Processor's obligation to report or respond to a Personal Data Breach under Sections 8.5 will not be construed as an acknowledgement by Processor of any fault or liability with respect to the Personal Data Breach.

10. Processor's Role as a Data Controller. The parties acknowledge and agree that to the extent Processor processes Personal Data in connection with the Agreement to: (i) monitor, prevent and detect fraud, and to prevent harm to Controller, Processor and the Processor's affiliates, and to third parties; (ii) comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Processor is subject; (iii) analyze, develop and improve Processor's products and Solutions; or (iv) provide the Processor Solutions to Processor users, Processor is acting as a data controller with respect to the Processing of such Personal Data it receives from or through Controller.

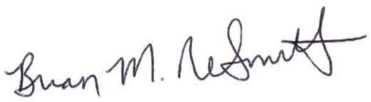
Controller	**Arctic Wolf Networks, Inc.**
Signature:_____	Signature: 
Customer Legal Name:_____	Print Name: Brian NeSmith
Print Name:	Title: CEO
Title:_____	
Date:_____	Notice Address: PO Box 46390, Eden Prairie, MN 55344
Notice Address:_____	Email: legal@arcticwolf.com
Email:_____	

EXHIBIT A

Details of Processing

Nature and Purpose of Processing: The Nature and Purpose of Processing as contemplated by this Data Processing Agreement shall be as set forth in the governing Solutions Agreement or equivalent agreement as executed by the Controller and Processor as it pertains to the delivery of Arctic Wolf Solutions to the Controller.

Duration of Processing: The Duration of Processing shall not exceed the term of the then-current Subscription as set forth on the applicable then-current Arctic Wolf Order Form or equivalent transaction document between either Controller and Processor or Controller and an Arctic Wolf Authorized Partner.

Categories of Data Subjects:

1. Controller corporate and contact information
2. Controller application users (admin users)
3. Clients of Controller's product or services
4. MSPs or Channel Partners
5. Employees of Controller
6. Individual information collected via website or sales/marketing activities

Type of Personal Data:

Contact information and information required to set up and perform the Solutions: names, email addresses, phone numbers, usernames, passwords, IP addresses, geolocation data, device ID.

Log data: In order to perform Solutions for Controller, via cloud monitoring and/or sensors installed with Controller, Processor receives free form log data and associated information in order to detect security issues. Such log data may include any category of personal data if Controller transmits such personal data to Processor. Log data is subject to redaction of identifiable personal data elements, and log data held on Processor's systems is routinely purged in accordance with the Agreement.

Exhibit B – Standard Contractual Clauses

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of Data Exporting organization: See signature page of the EU Data Processing Addendum

Address, Telephone, Email of Data Exporting Organization: See signature page of the EU Data Processing Addendum

(the "data exporter")

And

Arctic Wolf Networks, Inc.

8939 Columbine Road, Suite 150, Eden Prairie, MN 55347

(the "data importer)"

each a "party"; together "the parties"

HAVE AGREED on the following Contractual Clauses (the "Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1. **Definitions.** For the purposes of the Clauses:

(a) **"personal data"**, **"special categories of data"**, **"process/processing"**, **"controller"**, **"processor"**, **"data subject"**, and **"supervisory authority"** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) **"the data exporter"** means the controller who transfers the personal data;

(c) **"the data importer"** means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) **"the subprocessor"** means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) **"the applicable data protection law"** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) **"technical and organizational security measures"** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or

access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;

(g) **"personal data breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Clause 2. Details of the transfer. The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3. Third-party beneficiary clause.

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 9, Clause 10(2), and Clauses 11 to 14 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 9, Clause 10(2), and Clauses 11 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 9, Clause 10(2), and Clauses 11 to 14, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4. Obligations of the data exporter. The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 9(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 13 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5. Obligations of the data importer. The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that, in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 13;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6. Liability

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 13 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 13, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 13 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7. **Additional Safeguards Clauses**

1. These Additional Safeguards Clauses supplement, but do not vary or modify, the Standard Contractual Clauses.

2. To the greatest extent permissible under law applicable to data importer, data importer shall:

   (a) inform the data exporter about requests, orders or similar demands by a court, competent authority, law enforcement or other government body ("Law Enforcement Request") relating to the processing of personal data under these Clauses,

   (b) object to and challenge any Law Enforcement Request by taking legally available steps to not be compelled to disclose any personal data processed under these Clauses,

   (c) minimize any compelled transfer of personal data in response to a Law Enforcement Request to that specified in the applicable legal order. For purposes of this section, data importer would not be required to take actions that would result in civil or criminal penalty.

3. Data importer certifies that it has not purposefully created back doors or similar programming that could be used to access personal data processed under these Clauses on its systems, or purposefully created or changed its business processes in a manner that facilitates access to personal data processed under these Clauses on its systems by government authorities.

4. In case data importer makes personal data processed under these Clauses available to sub-processors, data importer will select sub-processors in a country outside of the European Economic Area that is not subject of an adequacy finding by the European Union Commission only after a due diligence that entails:

   (a) a review of any transparency reports made available by sub-processor,

   (b) and carrying out and documenting a transfer risk assessment prior to the engagement of sub-processor.

Clause 8. **Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 9. Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 10. Governing law. The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 11. Variation of the contract. The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 12. Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement, the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 13. Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name of Company:

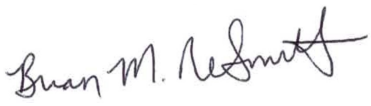
Printed name:

Position:

Date:

Signature…….

On behalf of the data importer:
Arctic Wolf Networks, Inc.
Printed Name: Brian NeSmith
Position: CEO

Signature: 

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer): the legal entity that has entered into an agreement with the data importer for the use of the data importer's cloud-based managed detection and response and managed risk solutions for the data exporter's internal business purposes.

Data importer
The data importer is Arctic Wolf Networks, Inc., a provider of managed data security solutions to data exporter.

Data subjects
The personal data transferred concern the following categories of data subjects:

Application users (admin users)

Data exporter's employees, contractors, agents, and other third parties

Categories of data
The personal data transferred concern the following categories of data:

Contact information and information required to set up and perform the Solutions: names, email addresses, postal address, phone numbers, user names, passwords, IP addresses, geolocation data, device ID.

Operational system log data, including, but not limited to operational values, event logs, and network data such as flow, HTTPS, TLS, DNS metadata, cursory inventory data, operating systems and versions, users and groups from Active Directory, system level inventory, event data, and network vulnerability data

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

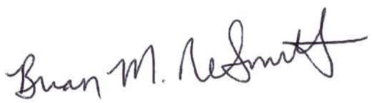
The personal data transferred should not contain special categories of data, unless provided by Data Exporter.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify): The processing is as set forth in the governing Solutions Agreement or equivalent agreement as executed by the Data Exporter and Data Importer as it pertains to the delivery of Data Importer Managed Detection and Response and Managed Risk Solutions to the Data Importer.

DATA EXPORTER
Name:……

Authorized Signature ……

DATA IMPORTER
Name: Arctic Wolf Networks, Inc.

Authorized Signature: 

Name/Title: Brian NeSmith, CEO

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4.4 and 5 (or document/legislation attached):

Data Importer's security efforts will include, without limitation (where applicable):

1. **Logical Access Controls**: Data Importer shall employ effective logical access control measures over all systems used to access, create, transmit, or process personal data, including but not limited to:
   a) User authentication must use unique identifiers ("**User ID's**") consistent with individual accountability and a complex password.
   b) Prohibition of clear-text credentials must be enforced.
   c) User access rights/privileges to information resources containing personal data must be granted on a need-to-know basis consistent with role-based authorization.
   d) User access must be removed immediately upon user separation or role transfer eliminating valid business need for continued access.
   e) Default passwords and security parameters must be changed in third-party products/applications used to support personal data and systems for the performance of the Solutions under the Solutions Agreement (the "Agreement").
   f) Two-factor authentication shall be used to secure all remote administrative access.

2. **Network Security Architecture:** Data Importer shall employ effective network security control measures over all systems used to create, transmit, or process personal data including but not limited to:
   a) Firewalls shall be operational at all times and shall be installed at the network perimeter between Data Importer's internal (private) and public (Internet) networks.
   b) Properly configured and monitored IDS/IPS (Intrusion Detection/Prevention Systems) must be used on Data Importer's network.
   c) Secure channels (e.g., SSL, SFTP, SSH, IPSEC, etc.) must be used at all times.

3. **Physical Security:** Data Importer shall maintain servers, databases, and other hardware and/or software components that store information related to Data Exporter's business activities in an access controlled and consistently monitored Data Center secured by appropriate alarm systems, which will not be commingled with another unrelated party's software or information. The facility storing personal data must follow best practices for infrastructure systems to include fire extinguishing, temperature control and employee safety.

4. **Risk Assessment/Audit:** At no additional cost Data Importer shall provide Data Exporter with results of a current security assessment by an accredited third party (e.g., SSAE 16-Type II reports, ISO 27001 certification, penetration test report etc.).

5. **Security Policy:** Data Importer maintains and enforces security policies consistent with all legal and privacy requirements applicable to Data Importer as a provider of the Solutions.

6. **Training and Awareness:** Data Importer shall provide necessary training to ensure security awareness in Data Importer personnel that are directly or indirectly engaged in handling personal data and systems for the performance of the Solutions, onsite or remotely.

7. **Protection of Customer Information**: In addition to what may be described in the Agreement, where applicable, Data Importer agrees to protect personal data as it would its own. For purposes of clarity, Data Importer agrees to adhere to the following controls surrounding the use and protection of personal data:
   a) Clear text (ftp, telnet, etc.) protocols may not be used to access or store personal data.
   b) personal data stored at rest must be encrypted with key sizes of 256-bit for symmetric and 2048-bit for asymmetric encryption.
   c) personal data may not be copied, sold or used for solicitation purposes by the Data Importer or its business partners. Personal data may only be used in conjunction with and within the scope of the Agreement.
   d) personal data must be segregated from other Data Importer customers, systems, or applications unrelated to Data Exporter.
   e) Data Importer must disclose where personal data will be stored and processed. Storage of personal data shall take place within the United States; however, personal data may be accessed in accordance with the terms of Section 10 of the Agreement.

8. **System Monitoring**: Data Importer shall regularly audit and monitor information systems processing of configured Data Exporter's business activities to ensure the protection of personal data. Data Importer must have defined processes for security alerting, escalation and remediation that are consistent with the Solutions procured pursuant to the Agreement.

9. **Vulnerability Management Controls**: Data Importer shall employ effective vulnerability management control measures over all of its systems used to perform the Solutions and that are used to create, transmit, or process personal data, including; but, not limited to:
   a) Conduct vulnerability scans of their network to ensure no critical security vulnerabilities remain unresolved post 30 days.
   b) Deploy and maintain currency of up-to-date commercially available anti-virus, anti-spam, anti-malware software on all information system components used for the purpose of managing personal data. Additionally, provide for regular scanning for viral infections and update virus signature files frequently.
   c) Maintain a standard patch management process and practice to ensure the protection of any devices used to access, process or store personal data.
   d) Within 72 hours of confirmed fraudulent or malicious activity occurring on the Data Importer Solution, to inform the Data Exporter team about the activity to the extent it results in or may result in an unauthorized use or disclosure of personal data. Any request by the Data Exporter team for information will be provided to Data Exporter within two hours, to the extent known by Data Importer.
   e) Any security breach that involves personal data must be reported to Data Exporter without unreasonable delay. Data Importer shall immediately perform a root cause analysis as well as provide detailed information about measures taken by the Data Importer to prevent future breaches. All efforts to rectify or resolve the situation must include subsequent and regular notification for the reported incident.
   f) Data Importer agrees to provide full cooperation with Data Exporter and in the event of a data breach involving personal data including, but not limited to: server log information showing network and application traffic.

10. **Data Destruction:** Data Importer shall ensure that residual magnetic, optical, or electrical representation of personal data that has been deleted may not be retrieved or reconstructed when storage media is transferred, become obsolete or is no longer usable or required by Data Exporter.
   - Data Importer data retention and destruction must comply with applicable laws or regulations.
   - personal data stored on Data Importer media (e.g., hard drive, optical discs, digital media, tapes, paper, etc.) must be rendered unreadable or unattainable using the NIST Guidelines for Media Sanitization (Special Pub 800-88), prior to the media being recycled, disposed of, or moved off-site.