EU Data Processing Addendum

PLEASE READ THIS ADDENDUM CAREFULLY BEFORE USING THE SOLUTIONS OFFERED BY ARCTIC WOLF NETWORKS, INC. ("PROCESSOR"). THIS ADDENDUM SHALL APPLY TO THE EXTENT ARCTIC WOLF IS A PROCESSOR OF PERSONAL DATA (DEFINED BELOW) THAT IS SUBJECT TO CERTAIN DATA PROTECTION LAWS (DEFINED BELOW). YOU OR THE ENTITY YOU REPRESENT ("CUSTOMER" OR "CONTROLLER") AGREE THAT YOU HAVE READ AND ACCEPT THE TERMS IN THIS ADDENDUM, WHICH SUPPLEMENT THE MASTER SOLUTIONS AGREEMENT OR OTHER EQUIVALENT CUSTOMER SUBSCRIPTION AGREEMENT ENTERED INTO BY AND BETWEEN YOU AND PROCESSOR (THE "AGREEMENT"). IF YOU ARE ACCESSING THE SOLUTIONS ON BEHALF OF YOUR EMPLOYER, YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO AGREE TO THESE TERMS ON ITS BEHALF AND THE RIGHT TO BIND YOUR EMPLOYER THERETO. IF EITHER YOU OR YOUR EMPLOYER DO NOT UNCONDITIONALLY AGREE TO ALL THE TERMS AND CONDITIONS OF THIS ADDENDUM, YOU HAVE NO RIGHT TO USE PROCESSOR'S SOLUTIONS.

1. Definitions

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, or (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.

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 in Exhibit C or (2) authorized by Controller to do so under Section 4.2 of this Addendum.

1.5 "Data Subject" means an identified or identifiable person to whom Personal Data relates.

1.6 "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.

1.7 "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.

1.8 "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.

1.9 "Privacy Shield Principles" means the Swiss-U.S. and EU-U.S. Privacy Shield Framework and Principles issued by the U.S. Department of Commerce, both available at https://www.privacyshield.gov/EU-US-Framework.

1.10 "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.

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

1.12 "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).

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

2. Processing of Data

2.1 The rights and obligations of the Controller with respect to this Processing are described herein. 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 General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR" and together, "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 it provides to Processor regarding the Processing of such Personal Data. 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. This Addendum does not apply to Personal Data for which Processor is a controller.

2.2   Processor shall not Process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this Addendum or any other documented instructions provided by Controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest and (iii) in violation of the GDPR. Controller hereby instructs Processor to Process Personal Data in accordance with the foregoing and as part of any Processing initiated by Controller in its use of the Solutions.

2.3   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.

2.4   Following completion of the Solutions, at Controller's choice, Processor shall return or delete the Personal Data, 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 12(1) of the Standard Contractual Clauses shall be provided by Processor to Controller only upon Controller's request.

3.   Authorized Employees

3.1   Processor shall take commercially reasonable steps to ensure the reliability and appropriate training of any Authorized Employee.

3.2   Processor shall ensure that all Authorized Employees are made aware of the confidential nature of Personal Data and have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement with Processor, any Personal Data except in accordance with their obligations in connection with the Solutios.

3.3   Processor shall take commercially reasonable steps to limit access to Personal Data to only Authorized Employees.

4.   Authorized Sub-Processors

4.1   Controller acknowledges and agrees that Processor may (1) engage its affiliates and the Authorized Sub-Processors listed in Exhibit C to this Addendum to access and Process Personal Data in connection with the Solutions and (2) from time to time engage additional third parties for the purpose of providing the Solutions, including without limitation the Processing of Personal Data. By way of this Addendum, Controller provides general written authorization to Processor to engage sub-processors as necessary to perform the Solutions.

4.2 A list of Processor's current Authorized Sub-Processors (the "List") will be made available to Controller at www.arcticwolf.com/terms/subprocessors. Such List which may be updated by Processor from time to time. The List provides a mechanism to subscribe to notifications of new Authorized Sub-Processors and Controller agrees to subscribe to such notifications. At least ten (10) days before enabling any third party other than 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 such an engagement on legitimate grounds by informing Processor in writing within ten (10) days of receipt of the aforementioned notice by Controller. Controller acknowledges that certain sub-processors are essential to providing the Solutions and that objecting to the use of a sub-processor may prevent Processor from offering the Solutions to 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 this Addendum. Termination shall not relieve Controller of any fees owed to Processor under the Agreement.

4.4   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.

4.5   Processor will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Processor under this Addendum with respect to the protection of Personal Data. In case an Authorized Sub-Processors fails to fulfill its data protection obligations under such written agreement with Processor, Processor will remain liable to Controller for the performance of the Authorized Sub-Processor's obligations under such agreement

4.6   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

6.1   The parties agree that Processor may transfer Personal Data processed under this Addendum outside the European Economic Area ("EEA") or Switzerland as necessary to provide the Solutions. If Processor transfers Personal Data protected under this Addendum to a jurisdiction for which the European Commission has not issued an adequacy decision, Processor will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

6.2   Where required, any transfer of Personal Data made subject to this Addendum to any countries which do not ensure an adequate level of data protection shall be undertaken by Processor through one of the following mechanisms: (a) in accordance with the Swiss-U.S. and EU-U.S. Privacy Shield Framework and Principles issued by the U.S. Department of Commerce, both available at https://www.privacyshield.gov/EU-US-Framework (the "Privacy Shield Principles"), or (b) if (a) is unavailable, Standard Contractual Clauses.

6.3   If transfers are made pursuant to 6.2(a), Processor self-certifies to, and complies with, the Swiss-U.S. and EU-U.S. Privacy Shield Frameworks, as administered by the U.S. Department of Commerce, and shall maintain such self-certification and compliance with respect to the Processing of Personal Data transferred from member states of the EEA or Switzerland to any countries which do not ensure an adequate level of data protection within the meaning of the laws and regulations of the foregoing countries for the duration of the Addendum.

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, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes 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   Processor shall, taking into account the nature of the Processing and the information available to Processor, provide Controller with reasonable cooperation and assistance where necessary for Controller to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, *provided that* Controller does not otherwise have access to the relevant information. Controller shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Processor.

8.2   Processor shall, taking into account the nature of the Processing and the information available to Processor, provide Controller with reasonable cooperation and assistance with respect to Controller's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Controller shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Processor.

8.3   Processor shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum, and retain such records for a period of three (3) years after the termination of the Agreement. Controller shall, with reasonable notice to Processor, 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 reasonable 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 12(2) of the Standard Contractual Clauses shall be carried out in accordance with this Section 8.4.

8.5   Processor shall immediately notify Controller if an instruction, in the Processor's opinion, infringes the Data Protection Laws or Supervisory Authority.

8.6   In the event of a Personal Data Breach, Processor shall, without undue delay, inform Controller of the Personal Data Breach and take such steps as Processor in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Processor's reasonable control).

8.7   In the event of a Personal Data Breach, Processor shall, taking into account the nature of the Processing and the information available to Processor, provide Controller with reasonable cooperation and assistance necessary for Controller to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.8   The obligations described in Sections 8.5 and 8.6 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 and 8.6 will not be construed as an acknowledgement by Processor of any fault or liability with respect to the Personal Data Breach.

9.   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:_____

Print Name:_____   Title:_____

Title:_____   Date:_____

Date:_____

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 Master 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, user names, 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.