# DATA PROCESSING ADDENDUM

(Last Updated: 09/27/2021)

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 Exhibit A (Standard Contractual Clauses).

**To accept this Addendum:**

1. **Complete the Customer information in the signature boxes and sign and date page 7;**
2. **Sign and date page 21 (Annex I to Standard Contractual Clauses); and**
3. **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 7 in Customer's signature box and the date when a signed copy of this Addendum is received by Arctic Wolf as described above.

# DATA PROCESSING ADDENDUM

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

**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"), applicable to the Processing of Personal Data under the Agreement.

1.7 "Data Protection Laws" means the laws and regulations of the United States, the European Union, the European Economic Area and/or their member states, Switzerland, and/or the United Kingdom as applicable to the Processing of the categories of Personal Data set forth in Section 2.4.6 of this Addendum, including but not limited to, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"), the United Kingdom Data Protection Act 2018 ("**UK GDPR**"), and the Swiss Federal Data Protection Act ("**FDPA**").

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 (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws, and is delivered by Customer to Arctic Wolf as part of the Solutions.

1.10 "Personal Data Breach" means a breach of Processor's 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 the controller to processor clauses for the transfer of Personal Data from the EEA to processors established in non-EEA countries that do not provide an adequate level of data protection approved by the European Commission Implementing Decision of 4 June 2021, as currently set out at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914 (Module Two: Transfer Controller to Processor) and attached hereto as Exhibit A.

1.15 "2010 Standard Contractual Clauses" means the clauses for the transfer of Personal Data from the EEA to processors established in non-EEA countries that do not provide an adequate level of data protection approved by European Commission Decision of 5 February 2010, as currently set out at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087.

1.16 "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.

1.17 "UK transitional arrangements" means any other valid transfer mechanism then in existence and approved by the UK Information Commissioner's Office.

**2. Processing of Data**

2.1 Scope and Roles of the Parties. This Addendum applies when Personal Data is processed by Arctic Wolf. 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. Unless otherwise specifically agreed to by Arctic Wolf, Personal Data may be Processed by Arctic Wolf and its authorized third-party service providers in the United States, UK, the EEA or other locations around the world provided that the transfer of Personal Data will comply with the provisions of this DPA. As between the parties, all Personal Data Processed under the terms of the Agreement shall remain the property of Customer. During the term of the Agreement, Arctic Wolf shall Process Personal Data in accordance with Customer's written instructions (unless expressly waived in a written requirement) and as permitted in the Agreement. In the event Arctic Wolf reasonably believes there is a conflict with any Data Protection Law and Customer's instructions, Arctic Wolf will inform Customer and the parties shall cooperate in good faith to resolve the conflict and achieve the goals of such instruction.

2.2 Controller's Processing of Personal Data. Controller shall, in its use of the Solutions, 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) how 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.

2.4 Details of the Processing. For purposes of Annex I of the Standard Contractual Clauses or Appendix 1 of the 2010 Standard Contractual Clauses, the parties agree:

2.4.1 **Data Exporter/Data Importer.** The data exporter is Customer and the data importer is Arctic Wolf Networks, Inc.

2.4.2 **Frequency of Transfer.** The frequency of transfer is continuous.

2.4.3 **Duration.** Arctic Wolf will delete Personal Data in accordance with the Data Privacy Law, the Agreement, and the provisions set forth in this Addendum (including the Standard Contractual Clauses and the 2010 Standard Contractual Clauses).

2.4.4 **Purpose of Processing.** The purpose of the Processing of Personal Data under this Addendum is the provision of the Solutions by Arctic Wolf to Customer in compliance with the Agreement.

2.4.5 **Nature of Processing.** The provision of managed detection and response and managed risk solutions as described in the Agreement and subscribed to by Controller from time-to-time.

2.4.6 **Type of Personal Data.** Customer may provide Arctic Wolf with names, email addresses, phone numbers, usernames, passwords, IP addresses, geolocation data, device ID, and other system log metadata which may include any category of Personal Data if Customer transmits such Personal Data to Arctic Wolf. There are no special categories of Personal Data.

2.4.7 **Categories of Data Subjects.** Data Subjects may include Controller's employees, contractors, agents, vendors, and customers.

2.4.8 **Authorized Subprocessors.** All details relating to Authorized Sub-processors are set forth in Section 5 of this Addendum. In addition, for purposes of Annex I of the Standard Contractual Clauses, the competent supervisory authority will be the Dutch Data Protection Authority.

2.4.9 **Annex II.** For the purposes of Appendix 2 of the 2010 Standard Contractual Clauses, the description of the technical and organizational security measures is described in the Agreement and Annex II of the Standard Contractual Clauses (the "IT Security Standards").

2.5 Deletion or Return of Personal Data. Following expiration or termination of the Agreement, 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. The parties agree that the certification of deletion of Personal Data that is described in Clause 8.5 of the Standard Contractual Clauses or Clause 12(1) of the 2010 Standard Contractual Clauses shall be provided by Arctic Wolf to Customer only upon Customer's request.

**3. Transfer Mechanism.** To the extent applicable, the Standard Contractual Clauses shall apply only to Processing of Personal Data that is directly or indirectly transferred from the EEA or Switzerland to any recipient in a country that is not recognized by the European Commission or the Swiss FDPIC as providing an adequate level of protection to personal data or not covered by a suitable framework for the protection of Personal Data. To the extent applicable, the 2010 Standard Contractual Clauses shall apply only to the Processing of Personal Data that is directly or indirectly transferred from the UK to any recipient in a country that is not recognized by the UK GDPR or UK Information Commissioner's Office ("UK ICO") as providing an adequate level of protection to personal data or not covered by a suitable framework for the protection of Personal Data; and for the sake of clarify, the reference to "EU Data Protection laws" in the 2010 Standard Contractual Clauses shall mean "UK GDPR", references to the "EU" or "Members States" shall mean "United Kingdom", and references to a "supervisory authority" shall mean the "Information Commissioner's Office". In the event the 2010 Standard Contractual clauses were to be invalidated by the UK ICO, each party agrees to enter into good faith negotiations to execute the UK transitional arrangements. The Parties agree that by executing this Addendum they are also executing the Standard Contractual Clauses and/or the 2010 Standard Contractual Clauses (whichever is applicable) together with the following additional terms:

3.1 Applicability. (a) The Standard Contractual Clauses apply only to (i) Customer as a Data Exporter and, (ii) any Customer Affiliates subject to the GDPR or FDPA, and are hereby incorporated by reference. (b) The 2010 Standard Contractual Clauses apply only to (i) Customer as a Data Exporter and, (ii) any Customer Affiliates subject to the UK GDPR, and are hereby incorporated by reference.

3.2 Instructions. This Addendum and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement or this Addendum (as the case may be) for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 8.1(a) of the Standard Contractual Clauses or Clause 5(a) of the 2010 Standard Contractual Clauses, the following is deemed an instruction by the Customer to Process Personal Data: (i) Processing in accordance with the Agreement; (ii) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

3.3 Sub-processors. Pursuant to Clause 9 of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Option 2: General Written Authorisation applies. Pursuant to Clause 9 of the Standard Contractual Clauses or Clause 5(h) of the 2010 Standard Contractual Clauses, (a) Customer acknowledges and expressly agrees that Arctic Wolf Affiliates and the Authorized Sub-processors may be sub-processors; and (b) Customer acknowledges and expressly agrees that Arctic Wolf may engage new sub-processors as described in Section 5 of this Addendum. The parties agree that sub-processing obligations pursuant to Clause 9(b) of the Standard Contractual Clauses or Clause 11 of the 2010 Standard Contractual Clauses shall be carried out in accordance with GDPR Article 28 or applicable provisions of the applicable Data Protection Law. The parties agree that the copies of the Authorized Sub-processors agreements that must be provided by Arctic Wolf to Customer pursuant to Clause 9(c) of the Standard Contractual Clauses or Clause 5(j) of the 2010 Standard Contractual Clauses may have all commercial and confidential information, or clauses unrelated to the Standard Contractual Clauses or 2010 Standard Contractual Clauses or their equivalent, redacted by Arctic Wolf beforehand; and, that such copies will be provided by Arctic Wolf, in a manner to be determined in its discretion, only upon written request by Customer.

**4. Audits.** The parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses, or Clause 5(f) and Clause 12(2) of the 2010 Standard Contractual Clauses, shall be carried out in accordance with Section 11 of this Addendum. To the extent the Standard Contractual Clauses or the 2010 Standard Contractual Clauses additionally require Arctic Wolf's facilities be submitted for inspection, Customer may contact Arctic Wolf through prior written notice to request an on-site audit of the procedures relevant to the protection of Customer Personal Data. Customer shall reimburse Arctic Wolf for any time expended for any such on-site audit at Arctic Wolf's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Arctic Wolf shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. Customer shall promptly notify Arctic Wolf with information regarding any noncompliance discovered during the course of an audit. For the avoidance of doubt, Customer's right to audit shall be subject to any limitations set forth in the IT Security Standards or the Agreement.

**5. Authorized Sub-Processors**

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

5.2 A list of Arctic Wolf's current Authorized Subprocessors (the "List") is available to Customer at https://arcticwolf.com/terms/sub-processors/, which may be updated by Arctic Wolf from time to time. Customer agrees to subscribe to receive notifications from the List of new Authorized Subprocessors. At least ten (10) days before enabling any third party other than current Authorized Subprocessors to access or participate in the Processing of Personal Data, Arctic Wolf will add such third party to the List. If Customer reasonably believes the Authorized Subprocessor cannot comply with the requirements of Section 5.4 below, Customer may reasonably object to the addition of any such third parties to the List by informing Arctic Wolf in writing within ten (10) days of receipt of the aforementioned notice by Customer.

5.3 If Customer objects to an engagement in accordance with Section 5.2, and Arctic Wolf cannot provide a commercially reasonable alternative within a reasonable period of time, Arctic Wolf may terminate the Agreement. Termination shall not relieve Customer of any fees owed to Arctic Wolf under the Agreement. This termination right is Customer's sole and exclusive remedy if Customer objects to any newly added Authorized Subprocessor. If Customer does not object to the engagement of a third party in accordance with Section 5.2 within ten (10) days of notice by Arctic Wolf that third party will be deemed an Authorized Subprocessors for the purposes of this Addendum.

5.4 Arctic Wolf will enter into a written agreement with each Authorized Subprocessors that requires the Authorized Subprocessor to (1) protect Personal Data to the same extent required by Arctic Wolf under this Addendum, and (2) be in compliance with Data Protection Laws. Arctic Wolf will remain liable to Customer for the non-performance of the Authorized Subprocessor's data protection obligations under such agreement.

5.5 Arctic Wolf will ensure that Authorized Subprocessors only access and use Personal Data in accordance with the terms of the Agreement (including this Addendum) and that they are bound by written obligations: (i) that require them to provide at least the level of data protection required by Data Protection Laws and by the Agreement; and (ii) where applicable, that impose the level of data protection required by the Standard Contractual Clauses. As of the Effective Date, Arctic Wolf has executed the 2010 Standard Contractual Clauses with its Authorized Subprocessors (including a Global Data Protection Agreement with its Affiliates). Arctic Wolf will use its best endeavors to execute the Standard Contractual Clauses with its Authorized Subprocessors (including its Affiliates) before December 27, 2022. In the event the 2010 Standard Contractual clauses were to be invalidated by the UK ICO, Arctic Wolf will use its best endeavors to execute the UK transitional arrangements with its Authorized Subprocessors (including its Affiliates) in a timely manner.

5.6 Arctic Wolf may replace an Authorized Subprocessor without advance notice where the reason for the change is outside of Arctic Wolf's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, Arctic Wolf will inform Customer of the replacement subprocessor as soon as possible following its appointment. Section 5.2 applies accordingly.

**6. 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 as set forth in the IT Security Standards and the

Agreement. Arctic Wolf will regularly monitor compliance with the IT Security Standards. Arctic Wolf will not intentionally decrease the IT Security Standards during the term of the Agreement.

**7. Rights of Data Subjects**

7.1 Arctic Wolf shall, to the extent permitted by law and in a manner consistent with the functionality of the Solutions and Arctic Wolf's role as a processor of Personal Data of Data Subjects, notify Customer 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 Arctic Wolf receives a Data Subject Request in relation to Customer's data, Arctic Wolf will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Solutions. Customer 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 Arctic Wolf, and for ensuring that a record of consent to Processing is maintained with respect to each Data Subject.

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

**8. Actions and Access Requests**

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

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

**9. Personal Data Breach.** After becoming aware of a Personal Data Breach of Customer's Personal Data Processed by Arctic Wolf or its Authorized Subprocessors, Arctic Wolf shall (i) inform Customer of the Personal Data Breach without undue delay; (ii) 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 Arctic Wolf's reasonable control; (iii) provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the Data Protection Laws relating to the Personal Data Breach; and (iv) provide Customer with details about the Personal Data Breach. The obligations described in this Sections 9.1 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer.

**10. Audits and Certifications.** Within thirty (30) days of Customer's written request, and no more than once annually and subject to the confidentiality obligations set forth in the Agreement (unless such information is reasonably required to be disclosed as a response to a Data Subject's inquiries under the Data Protection Law), Arctic Wolf shall make available to Customer (or a mutually agreed upon third-party auditor) information regarding Arctic Wolf's compliance with the obligations set forth in this Addendum, including reasonable documentation as further set forth in Annex II of the Standard Contractual Clauses. For the avoidance of doubt, (a) the scope of such audit shall be limited to documents and records allowing the verification of Arctic Wolf's compliance with the obligations set forth in this Addendum, (b) an audit in connection with this Section 11 shall not include financial documents or records of Arctic Wolf or any documents or records concerning other customers of Arctic Wolf, (c) if the parties have agreed to allow Customer to annually audit Arctic Wolf's IT Security Standards in the Agreement or otherwise, the rights set forth in this Section 11 do not provide Customer with an additional annual right to audit Arctic Wolf's IT Security Standards, and (d) Arctic Wolf may charge fees for an audit or review in connection with this Section 11. Arctic Wolf will provide Customer with further details of

any applicable fee, and the basis of its calculation, in advance of any such review or audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

**11. Liability.** Each party's liability for breaches of this Addendum shall be subject to the limitations and exclusions of liability set out in the Agreement. Either party's liability for a breach of this Addendum will be subject to the liability cap set out in the Agreement.

**12. Miscellaneous.**

12.1 Conflicts. In the event of any conflict or inconsistency between this Addendum and the Agreement, the terms of this Addendum shall prevail. In the event and to the extent of any conflict or inconsistency between the body of this Addendum and the Standard Contractual Clauses or the 2010 Standard Contractual Clauses in a way that materially affects the adequacy of the transfer, the Standard Contractual Clauses or the 2010 Standard Contractual Clauses shall prevail.

12.2 Severability. In the event any provision of this Addendum, in whole or in part, is invalid, unenforceable or in conflict with the applicable laws or regulations of any jurisdiction, such provision will be replaced, to the extent possible, with a provision which accomplishes the original business purposes of the provision in a valid and enforceable manner, and the remainder of this Addendum will remain unaffected and in full force.

12.3 Counterparts. This Addendum may be executed in several counterparts, each of which shall be deemed and original and all of which shall constitute one and the same instrument and shall become effective when counterparts have been signed by each of the parties and delivered to the other parties; it being understood that all parties need not sign the same counterparts. Signatures of the parties transmitted via facsimile or other electronic means shall be deemed to be their original signatures for all purposes.

| **Customer** | **Arctic Wolf Networks, Inc.** |
|---|---|
| Signature:_____ | Signature:  |
| Customer Legal Name:_____ | Print Name: Nick Schneider |
| Print Name: | Title: President & CEO |
| Title:_____ | |
| Date:_____ | Notice Address: PO Box 46390, Eden Prairie, MN 55344 |
| Notice Address:_____ | Email: legal@arcticwolf.com |
| Email:_____ | |

**Exhibit A**

**Standard Contractual Clauses**

**for the transfer of personal data outside the EEA**

## SECTION I

### *Clause 1*

### Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

### *Clause 2*

### Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

***Clause 3***

**Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

***Clause 4***

**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

***Clause 5***

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

***Clause 6***

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

### *Clause 7 – Optional*

### Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## SECTION II – OBLIGATIONS OF THE PARTIES

### *Clause 8*

### Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

### 8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

### 8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

### 8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### 8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

### 8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### 8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can

be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

### *Clause 9*

### Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

### *Clause 10*

### Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

### *Clause 11*

### Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([4]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

***Clause 12***

**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

***Clause 13***

**Supervision**

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

### *Clause 14*

### Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended

onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([5]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

***Clause 15***

**Obligations of the data importer in case of access by public authorities**

**15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the

country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

### *Clause 16*

**Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which

the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

### *Clause 17*

### Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

### *Clause 18*

### Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

## ANNEX I

### A. LIST OF PARTIES

**Data exporter(s):**

Data Exporter is the customer of Data Importer subscribing to the Solutions described in the Solutions Agreement executed by the parties for the delivery of managed detection and response and/or managed risk solutions.

Activities relevant to the data transferred under these Clauses:

Data Exporter is a provider of security operation solutions which processes Personal Data in the delivery of such solutions and requires the transfer of Personal Data to the US.

Signature and date: _____

Data Exporter's role is Controller.

**Data importer(s):**

Data Importer is Arctic Wolf Networks, Inc., a provider of security operations solutions.

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

Contact person's name, position and contact details:

IITR Cert GmbH
Dr. Sebastian Kraska, Data Protection Representative
Eschenrieder Str 62c, 82194 Groebenzell, Germany
email@iitr.de

Activities relevant to the data transferred under these Clauses:

Data Importer is a customer of Data Exporter and has contracted with Data Exporter for the delivery of Data Exporter's security operation solutions which may require the processing of Personal Data and transfer of Personal Data to the US.

Signature and date:  09/27/2021

Data Importer's role is Processor.

### B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose personal data is transferred*

Data Subjects include, but are not limited to, Solution users (Administrators), employees, contractors, agents, and other third parties

*Categories of personal data transferred*

Personal Data includes but is not limited to:

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

Operational system log data provided by Data Exporter to Data Importer for the delivery of the Solutions, 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

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

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

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

Personal Data is transferred on an ongoing basis for the term of the Agreement.

*Nature of the processing*

The processing is as set forth in the governing Agreement executed by the Data Exporter and Data Importer as it pertains to the delivery of Data Importer's Managed Detection and Response and Managed Risk Solutions to the Data Importer.

*Purpose(s) of the data transfer and further processing*

Data Importer processes the Personal Data in accordance with the instructions of the Data Exporter as set forth in the Agreement and the Data Protection Addendum.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

Contact information and information required to set up and perform the Solutions are retained during the Solutions subscription term for use in accordance with the Agreement.

Operational systems log data is retained for the retention period purchased by Data Exporter and returned or destroyed by Data Importer in accordance with the terms of the Agreement or as requested by Data Exporter.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

Subprocessors process Personal Data to permit Data Importer's delivery of the Solutions to Data Exporter in accordance with the terms of the Agreement and are subject to terms and conditions, including terms related to duration of processing, no less restrictive than those required of Data Importer pursuant to the terms of the Agreement. The purpose of processing is set forth on Data Importer's subprocessor list.

## C. COMPETENT SUPERVISORY AUTHORITY

*Identify the competent supervisory authority/ies in accordance with Clause 13*

Dutch Supervisory Authority

# ANNEX II

## TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Data Importer has implemented and will maintain the following security measures for the protection of Personal Data, which in conjunction with the security commitments in the DPA and the Solutions Agreement are Data Importer's responsibilities with respect to the security of Personal Data delivered by Data Exporter for Data Importer's delivery of the Solutions.

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 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 Personal Data**: 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.

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.
   a) Data Importer data retention and destruction must comply with applicable laws or regulations.
   b) 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.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.