

## **DATA PROCESSING ADDENDUM**

(Last Updated: November 2024)

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 “**Products**”) 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 Applicable Data Privacy Laws, as defined in the Addendum.

### **How to accept this Addendum**

This Addendum consists of the main terms and Schedules I through III.

To accept this Addendum, please execute where highlighted **yellow** on the pages listed below:

1. Complete the Customer information in the signature boxes and sign and date page 8;
2. Send the completed and signed Addendum to Arctic Wolf at [legal@arcticwolf.com](mailto: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 8 in Customer's signature box and the date when a signed copy of this Addendum is received by Arctic Wolf as described above.

## Arctic Wolf Data Processing Addendum – Frequently Asked Questions

Thank you for reviewing the Arctic Wolf Data Processing Addendum. We appreciate your interest in becoming a customer of Arctic Wolf. As a cybersecurity company, protecting our customers' personal information is a priority. We hope the below information will help you better understand how Arctic Wolf protects this information.

Please note that this information is not considered part of the contract at any time. This is provided for information purposes only.

### What is Arctic Wolf's role?

Arctic Wolf is processor as it relates to the delivery of our products and services (the "Products") to you. Arctic Wolf processes the personal information you provide to us in accordance with your instructions. You remain the controller of your information received in the delivery of the Products. You also may provide personal information to us that we use for billing, account management, and communication purposes. We use this information as a controller for such purposes.

### Your DPA only references European and United Kingdom privacy laws. Why?

Our DPA incorporates the core privacy principles that underlie many international data protection laws, and most significantly, the General Data Protection Regulation ("GDPR") from the European Economic Area and the United Kingdom, applicable state privacy laws which pertain to business to business transactions and specifically the California Privacy Rights Act of 2020 ("**CCPA**"), and other country specific privacy laws which apply to our operations, specifically the South Africa Protection of Personal Information Act ("**POPIA**"), the Australia Privacy Act No. 119 1988 (as amended), and the Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"). This foundation provides our global customers with a basis to support their privacy compliance requirements. However, our customers are responsible for determining whether our practices and this framework are sufficient to process personal information given our customers' integral knowledge of the legal and regulatory frameworks within which they operate.

### What data does Arctic Wolf receive to deliver the Products and what personal information may be included?

As a processor, and depending on the Products subscribed to (please see our Privacy Notice located at <https://arcticwolf.com/terms/privacy-notice-for-customers/> for further information), we may receive the following personal information from our customers:

- **Points of Contact Information.** Points of Contact Information includes contact details for the individuals who may be contacted by Arctic Wolf to deliver the Products. This Points of Contact Information will be collected by Arctic Wolf during various phases of Product delivery and throughout the life of the subscription. Points of Contact Information may include the following personal information: first name, last name, corporate email address, phone number, job title, address, organization hierarchy.
- **Solutions Data.** Solutions Data is systems and operational log data provided by our customers during the onboarding process as well as collected via the deployed MDR and MR Solutions. Personal information included in the Solutions Data may include: first name, last name, IP (Internet Protocol) Addresses, geolocation, usernames, passwords, email addresses. Arctic Wolf does not require any special categories of data to deliver these Solutions.
- **Incident Evidence.** Incident Evidence is the information you provide to Arctic Wolf and is required for the completion of the forensic/investigation processes conducted by Arctic Wolf as part of the incident response (IR) services. You provide this information to Arctic Wolf via firewall logs, server/workstation logs, logs from cloud services, email, individual files, full images of servers/workstations, SaaS configuration data, Firewall configuration data, memory snapshots, process lists, installed software lists, inventory of hosts, and DNS records. To the extent personal information is included in these sources of information, Arctic Wolf will obtain all such personal information to deliver IR services.
- **Learner Data.** Learner Data may be provided by you via the Administrator Portal or via a direct API feed from your Active Directory set up to Arctic Wolf with respect to the Users you permit to use the Managed Security Awareness Solution. Learner Data includes User setup details, including email, work title, and name and your program metrics, including your Users' learning status, training scores, and Phishing results associated with such Users' use of this Solution.
- **Phishtel Data.** Phishtel Data includes information pertaining to the phishing email(s) self-reported by a User as part of the Managed Security Awareness solution and includes or may include name of User, email of User, json web token, full content of email, and version data.
- **Security Profile Data.** Security Profile Data may be uploaded by you or your third-party agent in the Cyber JumpStart Portal when using the modules therein. Personal information you may elect to upload into the applications includes names, emails, employee and third-party agent contact information, and IP addresses.

### Does Arctic Wolf use subprocessors?

Arctic Wolf uses subprocessors to provide the Products (e.g., as part of our global follow-the-sun operations to make updates to our software-as-a-service applications and prevent or address technical issues). Any subprocessor that Arctic Wolf engages to process our customers' personal information undergoes a thorough vendor due diligence review and agrees to abide by data protection terms no less protective than those set forth in this DPA.

**Who are Arctic Wolf's subprocessors?**

A list of Arctic Wolf's subprocessors can be found [here](#).

**How do you inform your customers about new subprocessors?**

Arctic Wolf will update its subprocessor list at least ten (10) days prior to implementing a new subprocessor. Customers can subscribe to receiving an alert that the list has been updated. Our customers are responsible for ensuring that the people in their organization who need to be notified about such updates subscribe to changes to the subprocessor list.

**Can customers object to Arctic Wolf's use of a new subprocessor?**

Where required by law, Arctic Wolf's customers can object to use of a new subprocessor on reasonable grounds relating to data protection. If Arctic Wolf decides to retain a subprocessor to which a customer has objected, then the customer has the option to terminate the affected Product.

**How does Arctic Wolf help its customers legalize cross-border data transfers of personal information and meet the "adequacy" requirements for the United Kingdom, Switzerland, and European Economic Area?**

Arctic Wolf has self-certified under the EU-U.S. Data Privacy Framework, the UK Extension related thereto, and the Swiss-U.S. Data Privacy Framework Principles and commits to the EU-U.S. Data Privacy Framework Principles as described therein. In addition, we use Standard Contractual Clauses to legalize transfers of personal information outside of the European Economic Area, the United Kingdom and Switzerland and within this DPA, we include reference to the Standard Contractual Clauses 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](https://eur-lex.europa.eu/eli/dec_impl/2021/914) (Module Two: Transfer Controller to Processor) and, with respect to UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses published by the UK's Information Commissioner's Office UK version B1.0, dated March 21, 2022. These Standard Contractual Clauses are model contracts developed by the European Commission and UK Information Commissioner's Office to legalize transfers of personal data from the United Kingdom, Switzerland and European Economic Area to processors located in other countries.

**(For information purposes only, this FAQ does not form part of any contract)**

## DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**Addendum**”) forms part and is incorporated into the agreement between Arctic Wolf Networks, Inc. and Customer for the purchase of or subscription to the Products identified in the agreement between Customer and Arctic Wolf (jointly referred to as the “**Agreement**”). Each of Customer and Arctic Wolf may be referred to herein as a “**party**” and together the “**parties**”.

By signing below, Customer enters into this Addendum on behalf of itself and, to the extent required under Data Protection Laws (defined hereinafter), in the name and on behalf of its Authorized Affiliates, if and to the extent Arctic Wolf Processes Personal Data for such Affiliates and they qualify as, for the purposes of the GDPR, the controller and, for the purposes of the CCPA, the business (or as such similar terms are used under Data Protection Laws). For the purposes of the GDPR, Arctic Wolf is the processor and, for the purposes of the CCPA, the service provider (or as such similar terms are used under Data Protection Laws). In the delivery of Products to Customer pursuant to the Agreement, Arctic Wolf may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

**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 “Authorized Sub-Processor” means those parties listed in Schedule II of this Addendum, as such list may be updated from time-to-time in accordance with Section 5, who have a need to know or otherwise access Personal Data to enable Processor to perform its obligations under this Addendum or the Agreement and do not include subcontractors who provide ancillary services such as telecommunication services, postal/transport services, maintenance and user support services, as well as other resources, tools, and measures to ensure the confidentiality, availability, integrity and resilience of the Products.

1.3 “Customer” means the customer entity that is party to the Agreement.

1.4 “Data Subject” means (i) “data subject” as defined under the GDPR or the UK GDPR, (ii) “consumer” or “household” as defined under the CCPA, and/or (iii) such similar term under the relevant Data Protection Laws.

1.5 “Data Protection Laws” means one or more of the following data protection laws or regulations as applicable to the Processing of Personal Data by Arctic Wolf under this Agreement: (i) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (“**GDPR**”); (ii) the United Kingdom (“**UK**”) Data Protection Act 2018 and the UK General Data Protection Regulation (“**UK GDPR**”); (iii) Swiss Federal Data Protection Act on Data Protection of 25. September 2020 (Status as of 1. September 2023) (“**FDPA**”); (iv) California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (“**CCPA**”); (v) the South Africa Protection of Personal Information Act (“**POPIA**”); (vi) the Australia Privacy Act No. 119 1988 (as amended); (vii) Canadian Personal Information Protection and Electronic Documents Act (“**PIPEDA**”); and (viii) any relevant law, statute, regulation, legislative enactment, order or other binding instrument, that implements, supplements, or amends the foregoing.

1.6 “EU 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 (EU) 2021/914 of 4 June 2021, as currently set out at: [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX:32021D0914](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914) (Module Two: Transfer Controller to Processor) as may be amended or replaced by the European Union from time-to-time.

1.7 “EEA” means the European Economic Area.

1.8 “Instruction” means the (i) instructions from Customer as set forth in the Agreement, (ii) the “Business Purpose” as defined under CCPA, (iii) such similar term under the relevant Data Privacy Laws, and/or (iv) any 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 (i) “personal data” as defined under the GDPR and/or the UK GDPR, (ii) “personal information” as defined under CCPA, and/or (iii) such similar term under the relevant Data Protection Laws, that is under the control of Customer and Processed by Arctic Wolf in connection with the delivery of the Products.

1.10 “Personal Data Breach” means a breach of Processor’s security leading to the accidental or unlawful or unauthorized destruction, loss, alteration, encryption, unavailability, acquisition, disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

1.11 “Process” or “Processing” is as defined under the applicable Data Privacy Laws and further described in Schedule I.

1.12 “Restricted Transfer” means the disclosure, grant of access or other transfer of Personal Data Processed under the Agreement to any person located in Third Countries.

1.13 “Products” shall have the meaning set forth in the Agreement.

1.14 “Sale”, “Sell” or “Selling” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data with a Third Party, whether for monetary or other valuable considerations or for no consideration, for the Third Party’s commercial purposes.

1.15 “Standard Contractual Clauses” means government approved contract mechanism for Restricted Transfers.

1.16 “Third Country(ies)” means countries outside of the scope of the data protection laws of the EEA, Switzerland, and/or the UK (as applicable), excluding countries approved as providing adequate protection for Personal Data by the European Commission and/or the Information Commissioner’s Office (as applicable) from time-to-time.

1.17 “Third Party” means any person (including companies, entities, organizations, etc.) that is not Customer, an Authorized Subprocessor, or Arctic Wolf.

1.18 “UK Standard Contractual Clauses” means the International Data Transfer Addendum issued by the UK’s Information Commissioner’s Office under s.119(A) of the UK Data Protection Act 2018 as may be updated from time-to-time, and currently found at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>.

1.19 “Regulator” means (i) in the context of the EEA and the EU GDPR, the meaning given to that term in the EU GDPR; (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner’s Office; and (iii) in the context of Switzerland means Swiss Federal Data Protection and Information Commissioner; and (iv) in the context of any other jurisdiction, any governmental authority with jurisdiction over Customer’s Processing of Personal Data under the Agreement.

## **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 acknowledge and agree that, regarding the Processing of Customer’s 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, and unless otherwise determined by a Regulator. 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 Instructions (unless expressly waived in a written requirement). Further information regarding Arctic Wolf’s Processing can be found in Schedule II. In the event Arctic Wolf reasonably believes there is a conflict with any Data Protection Laws 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 Products, Process Personal Data and provide Instructions for the Processing of Personal Data in compliance with the Data Protection Laws. Controller shall ensure that Controller’s 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, (iii) the volume, categories, and sensitivities of the Personal Data provided to Processor, and (iv) 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 Products and shall indemnify Processor from all claims and losses in connection therewith.

2.3 CCPA. If the CCPA is applicable,

2.3.1 Arctic Wolf shall act as a “service provider” and certifies that it shall Process Customer Personal Data on behalf of Customer in accordance with and for the Business Purpose. Notwithstanding the foregoing, Arctic Wolf may Process Customer Personal Data as may otherwise be permitted for service providers or under a comparable exemption from “Sale” under Data Protection Laws, as reasonably determined by Arctic Wolf.

2.3.2 Each party shall comply with the obligations applicable to that party under the applicable Data Protection Laws.

2.3.3 Arctic Wolf represents and warrants that: (i) it shall promptly inform Customer if, in Arctic Wolf’s opinion: (i) Arctic Wolf cannot comply with such Data Protection Law, or (ii) Customer’s Instructions violate such Data Protection Law, provided that Arctic Wolf is not obliged to perform a comprehensive legal examination with respect to an Instruction of Customer; (iii) its personnel and Authorized Subprocessors who Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and (iv) Arctic Wolf understands the restrictions placed on it as a Processor of the Personal Data.

2.3.4 Customer represents and warrants that: (i) its use of the Products and the Instructions provided do not contravene such Data Protection Law; (ii) it has complied and continues to comply with such Data Protection Law, in particular that it has obtained any necessary consents and/or given any necessary notices, and/or otherwise has the right to disclose Personal Data to Arctic Wolf and enable the Processing set out in this Addendum and as contemplated by the Agreement; (iii) it has assessed the requirements under such Data Protection Law as they apply to Customer with regard to Personal Data and finds that the security measures referenced in Schedule 3 are adequate to meet those requirements; and (iv) it will ensure compliance with and shall not in any way alter or diminish such security measures referenced in Schedule 3 to the extent applicable to Customer through its use of the Products.

2.4 Restricted Transfers.

2.4.1 Arctic Wolf has self-certified under the EU-U.S. Data Privacy Framework, the UK Extension related thereto, and the Swiss-U.S. Data Privacy Framework Principles and commits to the EU-U.S. Data Privacy Framework Principles and/or the Swiss-US Data Privacy Framework (as applicable) as described therein.

2.4.2 To the extent needed and applicable, if, in fulfilling its obligations under the Agreement or pursuant to other lawful instructions from Customer, there is a Restricted Transfer of Personal Data, the parties agree to enter into and abide by the EU Standard Contractual Clauses and/or UK Addendum (as applicable), which are incorporated into this Addendum as follows:

- (i) Customer is the Data Exporter and Arctic Wolf is the Data Importer (the foregoing shall apply with respect to Table 1 of the UK Addendum);
- (ii) In Clause 7, the "Docking Clause (Optional)", shall be deemed incorporated (the foregoing shall apply with respect to Table 1 of the UK Addendum);
- (iii) In Clause 9, the parties choose Option 2, 'General Written Authorisation', with a time period of 10 days (the foregoing shall apply with respect to Table 2 of the UK Addendum);
- (iv) The optional wording in Clause 11 shall be deemed not incorporated (the foregoing shall apply with respect to Table 2 of the UK Addendum);
- (v) In Clause 13, the competent Regulator shall be the Irish Data Protection Authority;
- (vi) In Clause 17, the Data Exporter and Data Importer agree that the EU Standard Contractual Clauses shall be governed by the laws of Ireland, and choose Option 1 to this effect (Part 2, Section 15(m) of the UK Addendum shall apply);
- (vii) In Clause 18, the Data Exporter and Data Importer agree that any disputes shall be resolved by the courts of Ireland (Part 2, Section 15(n) of the UK Addendum shall apply);
- (viii) In accordance with Section 19 of the UK Addendum and Section 2.6 of this Addendum, neither party may end the UK Addendum when the UK Addendum changes;
- (ix) Completed Annexes I, II and III of the EU Standard Contractual Clauses and Annexes 1B, II and III of Table 3 of the UK Addendum are included in Annexes I through III herein;
- (x) Notwithstanding the fact that the Standard Contractual Clauses are incorporated herein by reference without the Standard Contractual Clauses actually being signed by the parties, the parties agree that the execution of this Addendum is deemed to constitute its execution of the Standard Contractual Clauses on behalf of the Data Exporter or Data Importer (as applicable), and that it is duly authorized to do so on behalf of, and to contractually bind, the Data Exporter or Data Importer (as applicable) accordingly;
- (xi) The parties agree that the Standard Contractual Clauses shall cease to apply to the Processing of Personal Data if and to the extent that the relevant transfer of Personal Data ceases to be a "restricted transfer"; and
- (xii) The provisions in this Addendum shall be without prejudice to the parties' ability to rely on any other legally valid international data transfer mechanism for the transfer of data out of the EEA, UK, and/or Switzerland. The parties agree to enter into other standard contractual clauses approved under Data Protection Laws to effectuate the Restricted Transfers of Personal Data for purposes of providing the Products.

2.5 The parties further agree that if any of the EU Standard Contractual Clauses or the UK Addendum are updated, replaced, or are no longer available for any reason, the parties will cooperate in good faith to implement updated or replacement Standard Contractual Clauses, as appropriate, or identify an alternative mechanism(s) to authorize the contemplated Restricted Transfers.

2.6 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 UK Standard Contractual Clauses shall be provided by Arctic Wolf to Customer only upon Customer's request.

**3. Audits.** Taking into account the nature of the Processing and the information available to Arctic Wolf, Arctic Wolf shall provide reasonable assistance in response to inquiries from Customer or a competent Regulator relating to Arctic Wolf's Processing of Customer's Personal Data.

3.1 Arctic Wolf shall, upon written request from Customer, provide Customer with information reasonably necessary to demonstrate compliance with its obligations set forth in this Addendum. This information shall consist of permitting examination of the most recent reports, certificates and/or extracts prepared by an independent auditor pursuant to Arctic Wolf's ISO27001 or similarly held industry certification.

3.2 In the event the information provided in accordance with Section 3.1 above is insufficient to reasonably demonstrate compliance, Arctic Wolf shall permit Customer, or Customer's third party auditor (provided such auditor is not a competitor to Arctic Wolf or provides products and/or services to a competitor of Arctic Wolf) to inspect or audit the technical and organisational measures of Arctic Wolf for the purposes of monitoring compliance with Arctic Wolf's obligations under this Addendum. Any such audit or inspection shall be: (i) at Customer's expense; (ii) limited in scope to matters specific to Customer; (iii) agreed in advance between the parties in writing, including scope, duration, start date and Arctic Wolf's then-current rates for professional services; (iv) conducted in a way that does not interfere with Arctic Wolf's day-to-day business; (v) during local business hours of Arctic Wolf and, upon not less than twenty (20) business days advance written notice unless, in Customer's reasonable belief an identifiable, material Breach has arisen; (vi) limited to no more than once per any twelve (12) calendar month period, except if (i) required by instruction of a competent Regulator; or (ii) in case of a security breach; and (vii) subject to the confidentiality obligations in the Agreement or, where a third-party auditor conducts the audit, such third-party auditor must be a professional bound by a duty of confidentiality or subject to a suitable non-disclosure agreement.

3.3 Customer will provide Arctic Wolf with copies of any audit reports generated in connection with any audit under this Section, unless prohibited by the applicable Data Protection Law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this Addendum.

3.4 For the avoidance of doubt, the provisions of this Section 3 shall also apply to the audit provisions of any Standard Contractual Clauses entered into in accordance with Section 2 of this Addendum.

#### **4. Authorized Sub-Processors**

4.1 Customer consents to the use of Authorized Subprocessors to deliver the Products.

4.2 Customer agrees it may subscribe to receive notifications related to the modification to the 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 Authorized Subprocessor list referenced in Schedule III. If Customer reasonably believes the third party cannot comply with the requirements this Addendum, 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. If Customer objects to such change, and Arctic Wolf cannot provide a commercially reasonable alternative within a reasonable period of time, the parties 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 within ten (10) days of notice by Arctic Wolf that third party will be deemed an Authorized Subprocessors for the purposes of this Addendum.

4.3 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.

4.4 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 4.2 applies accordingly.

**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 as set forth in Schedule III. Arctic Wolf will regularly monitor compliance with such security standards and will not intentionally decrease the security standards during the term of the Agreement.

## **6. Rights of Data Subjects**

6.1 If Arctic Wolf directly receives a Data Subject Request in relation to Customer's Personal Data and Customer is identified or identifiable from the request without the need for any independent investigation that Customer is the applicable controller of such Data Subject's Personal Data, Arctic Wolf will promptly forward such Data Subject to Customer, unless otherwise required by the applicable Data Protection Law. If Arctic Wolf is legally compelled to respond directly to the Data Subject, Customer will fully co-operate with Arctic Wolf, as appropriate. Customer agrees that provision of technical tools to enable Customer to take the necessary action to comply with such requests shall be sufficient to discharge Arctic Wolf's obligations of assistance hereunder. 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.

6.2 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 a 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.

## **7. Actions and Access Requests**

7.1 Where Customer is obligated by Data Protection Laws to carry out a data protection impact assessment ("DPIA") relating to Customer's use of the Products, 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.

7.2 Arctic Wolf shall provide Customer with reasonable assistance to Customer in cooperation or prior consultation with any Regulator 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.

**8. Personal Data Breach.** After declaring a breach of security which results in or is likely to result in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer's Personal Data which affects the integrity, availability, or confidentiality of Customer's Personal Data (a "Breach") Processed by Arctic Wolf or its Authorized Subprocessors, Arctic Wolf shall (i) notify Customer of the Personal Data Breach without undue delay (and in no event more than seventy-two (72) hours); (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 applicable 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 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. For the avoidance of doubt, a Breach will not include unsuccessful attempts to, or activities that do not, compromise the security of Personal Data including, without limitation, unsuccessful log in attempts, denial of service attacks and other attacks on firewalls or networked systems and no notice of the foregoing shall be required. In the event a Breach requires notification by Customer to Data Subjects or relevant Regulators, the parties agree to coordinate in good faith on developing the content of any public statements or required notices.

**9. 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. Each party's liability for a breach of this Addendum will be subject to the liability cap set out in the Agreement. Without limiting the



parties' obligations under the Agreement, each party agrees that any regulatory penalties incurred by one party (the "Incurring Party") in relation to the Customer Personal Data that arise as a result of, or in connection with, the other party's failure to comply with its obligations under this Addendum or any applicable Data Protection Laws shall count toward and reduce the Incurring Party's liability under the Agreement as if it were liability to the other party under the Agreement.

**10. Changes in Data Protection Laws.** The parties agree to negotiate in good faith modifications to this Addendum if changes are required for Arctic Wolf to continue to Process Personal Data in compliance with Data Protection Laws, including but not limited to (i) the GDPR; (ii) the CCPA; (iii) any Standard Contractual Clauses; or (iv) if changes to the membership status of a country in the European Union or the European Economic Area require such modification.

**11. Confidentiality.** The confidentiality terms in the Agreement shall apply to this Addendum and where applicable, the Standard Contractual Clauses.


**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 UK Standard Contractual Clauses in a way that materially affects the adequacy of the transfer, the Standard Contractual Clauses or the UK 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.

**12.2.1 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.

**IN WITNESS WHEREOF,** the parties have caused this Addendum to be executed by their duly authorized representatives on the Effective Date.

<b>Arctic Wolf Networks, Inc.:</b>	<b>Customer Legal Name:</b>
<b>Signed:</b> 	<b>Signed:</b>
<b>Name:</b> <u>Andrew Hill</u>	<b>Name:</b> _____
<b>Title:</b> <u>Chief Legal Officer &amp; General Counsel</u>	<b>Title:</b> _____
<b>Date:</b> <u>11/01/2024</u>	<b>Date:</b> _____
<b>Notice Address:</b> PO Box 46390 Eden Prairie, MN 55344 Attn: General Counsel legal@arcticwolf.com	<b>Notice Address/email:</b>



## **SCHEDULE I TO DATA PROCESSING ADDENDUM**

### **Processing Details**

The details of the Processing relevant to the Products provided by Arctic Wolf can be found at <https://arcticwolf.com/terms/processing-details/>.

**SCHEDULE II  
TO DATA PROCESSING ADDENDUM**

Arctic Wolf maintains a list of its Authorized Subprocessors by Product at <https://arcticwolf.com/terms/sub-processors/>.

### **SCHEDULE III**

#### **Technical and Organisational Measures**

Arctic Wolf shall implement the technical and organisational security measures specified in its Product - Technical and Organizational Measures document set forth at <https://arcticwolf.com/terms/product-technical-measures/> as a minimum security standard. Customer acknowledges and agrees that the nature of the Products mean that the technical and organisational measures may be updated by Arctic Wolf from time-to-time, but such updates shall not result in a lesser standard of security to that in place upon signature of this Addendum.