ARIA Cybersecurity - Product End User License Agreement Terms and Conditions

This End User License Agreement Terms and Conditions (this "**Agreement**") is made and shall become effective as of the date of the Purchase Order (the "**Effective Date**"), by the End User Customer, referred to as the "**Customer**", and ARIA Cybersecurity a Delaware Corporation ("**ARIA Cybersecurity**"), pursuant to which ARIA Cybersecurity will provide to Customer the software applications described in the quote and/or in any provided Statement of Work. Customer and ARIA Cybersecurity may be referred to each as a "**Party**" or collectively as the "**Parties**".

In consideration of the obligations herein and other consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

1. Definitions.

"Affiliate" means any entity that a party directly or indirectly controls (e.g., subsidiary) or is controlled by (e.g., parent), or with which it is under common control (e.g., sibling).

"Agreement" means these ARIA Cybersecurity Terms and Conditions together with each Order.

"API" means an application program (or programming) interface.

"ARIA Cybersecurity data" shall mean the data generated by the ARIA Cybersecurity Offerings, including but not limited to, correlative and/or contextual data, and/or detections. For the avoidance of doubt, ARIA Cybersecurity Data does not include Customer Data.

"ARIA Cybersecurity Product" means any ARIA Cybersecurity proprietary software-as-a-service, software, hardware, supplied to for the use by the end user Customer. Such products may be used within an ARIA provided "Managed Service" which has additional terms conditions. ARIA provided "Professional Services", which may be specified in the applicable SOW will have additional SOW specific terms and conditions.

"Customer Contractor" means any individual or entity (other than an ARIA Cybersecurity Competitor) that: (i) has access or use of a Product under this Agreement solely on behalf of and for Customer's Internal Use, (ii) has an agreement to provide Customer (or its Affiliates) services, and (iii) is subject to confidentiality obligations covering ARIA Cybersecurity's Confidential Information.

"Customer Contractor Services" means products, services or content developed or provided by Customer Contractors, including, but not limited to, third party applications complimentary to the Offerings, implementation services, managed services, training, technical support, or other consulting services related to, or in conjunction with, the Offerings.

"Documentation" means ARIA Cybersecurity's end-user technical documentation included in the applicable Offering.

"Endpoint" means any physical or virtual device, such as, a computer, server, laptop, desktop computer, mobile, cellular, container or virtual machine image.

"Error" means a reproducible failure of a Product to perform in substantial conformity with its applicable Documentation.

“Internal Use” means access or use solely for Customer’s, own internal information security purposes. By way of example and not limitation, Internal Use does not include access or use: (i) for the benefit of any person or entity other than Customer or its Affiliates, or (ii) in any event, for the development of any product or service. Internal Use is limited to access and use by Customer and its Affiliates’ employees and Customer Contractors (except as set forth in the Section entitled Customer Contractors), in either event, solely on your behalf and for Customer’s benefit.

“Offerings” means, collectively, any Products, Product-Related Services, or Managed Services.

“Order” means any purchase order or other ordering document (including any SOW) accepted by ARIA Cybersecurity or a reseller that identifies the following ordered by Customer: Offering, Offering quantity based on ARIA Cybersecurity’s applicable license metrics (e.g., number of Endpoints, size of company (based on number of employees), number of Internet (IP) addresses), price and Subscription/Order Term.

“Product” means any of ARIA Cybersecurity’s cloud-based software or other products ordered by Customer as set forth in the relevant Order, the available accompanying API’s, the ARIA Cybersecurity Data, any Documentation and any Updates thereto that may be made available to Customer from time to time by ARIA Cybersecurity.

“Reseller” means an ARIA Cybersecurity authorized reseller who as an independent entity offers ARIA products and Managed services for resale and may at its discretion offer it in conjunction with their own or other 3Rd party products or services. ARIA Cybersecurity has no liability for and makes no warranties over such combined offerings.

“Subscription Order Term” means the period of time set forth in the applicable Order during which Customer is authorized by ARIA Cybersecurity to access and use the Product or Product-Related Managed Service, These subscription based orders are based for a specified order term and unless specified otherwise, automatically terminate at the end of the term for unless Customer provides a written notice 30 days prior to the end of the term its intent to renew or extend for an additional one year term.

“Support Service” Are optional subscription services where the customer requires additional ongoing product support beyond the initial time limited term up period when purchasing a standard product subscription.

“Updates” means any correction, update, upgrade, patch, or other modification or addition made by ARIA Cybersecurity to any Product and provided to Customer by ARIA Cybersecurity from time to time on an as available basis.

2. Affiliates, Orders and Payment.

2.1 Orders. Orders cannot be canceled once licenses are activated. Only those transaction-specific terms stating the Offerings ordered, quantity, price, payment terms, Subscription/Order Term, and billing/provisioning contact information will have effect (and for the avoidance of doubt, specifically excluding any pre-printed terms on a Customer or reseller purchase order), except if mutually agreed upon by ARIA Cybersecurity and Customer (or the applicable reseller).

2.2 Payment. Customer will pay the fees for Offerings to a reseller or ARIA Cybersecurity as set forth in the applicable Order. Unless otherwise expressly set forth as mutually agreed on the Order,

Customer will pay the fees and amounts stated on each Order within 30 days after receipt of the applicable invoice. Customer shall be responsible to pay any applicable sales, use, value added, withholding, import duties and other taxes, however designated, except for taxes based on ARIA Cybersecurity's income or with respect to ARIA Cybersecurity's employment of its employees

3. Access & Use Rights.

3.1 Evaluation. If ARIA Cybersecurity approves Customer's evaluation use of an ARIA Cybersecurity product ("Evaluation Product"), the terms herein apply to evaluation access and use of such Evaluation Product, except for the following different or additional terms: (i) the duration of the evaluation is as mutually agreed upon by you and ARIA Cybersecurity, provided that either ARIA Cybersecurity or you can terminate the evaluation at any time upon written (including email) notice to the other party; (ii) the Evaluation Product is provided "AS-IS" without warranty of any kind, and ARIA Cybersecurity disclaims all warranties, support obligations, and other liabilities and obligations for the Evaluation Product; and (iii) Customer's access and use is limited to Internal Use by Customer employees only.

3.2 Access & Use Rights. Subject to the terms and conditions of this Agreement (including ARIA Cybersecurity's receipt of applicable fees), ARIA Cybersecurity grants Customer, , a non-exclusive, non-transferable (except as expressly provided in the Section entitled Assignment), non-sublicensable license to access and use the Products in accordance with applicable Documentation solely for Customer's Internal Use during the applicable Subscription/Order Term. Customer's access and use is limited to the quantity in the applicable Order. Furthermore, the following additional terms and conditions apply to specific Products (or components thereof):

(a) Products with Software Components. If Customer purchases a subscription to a Product with a downloadable object-code component ("Software Component"), Customer may, during the Subscription/Order Term install and run multiple copies of the Software Components solely for Customer's and its Affiliates' Internal Use up to the maximum quantity in the applicable Order.

(b) ARIA Cybersecurity Tools. If ARIA Cybersecurity provides ARIA Cybersecurity Tools to Customer pursuant to performing Product Related Services, the license set forth in the Section entitled Access & Use Rights applies to such ARIA Cybersecurity Tools. Not all Services engagements will involve the use of ARIA Cybersecurity Tools.

3.3 Restrictions. The access and use rights set forth in this Section do not include any rights to(i) employ or authorize an ARIA Cybersecurity Competitor to (a) use or view the Offering or Documentation, or (b) provide management, hosting, or support for an Offering; (ii) alter, publicly display, translate, create derivative works of or otherwise modify an Offering; (iii) sublicense, distribute or otherwise transfer an Offering to any third party (except as expressly provided in the Section entitled Assignment); (iv) allow third parties to access or use an Offering (except for Customer Contractors as expressly permitted herein); (v) create public Internet "links" to an Offering or "frame" or "mirror" any Offering content on any other server or wireless or Internet-based device; (vi) reverse engineer, decompile, disassemble or otherwise attempt to derive the source code (if any) for an Offering (except to the extent that such prohibition is expressly precluded by applicable law), circumvent its functions, or attempt to gain unauthorized access to an Offering or its related systems or networks; (vii) use an Offering to circumvent the security of another party's network/information, develop malware, unauthorized surreptitious surveillance, data modification, data exfiltration, data ransom or data destruction; (viii) remove or alter any notice of proprietary right appearing on an Offering; (ix) conduct any stress tests, competitive benchmarking

or analysis on, or publish any performance data of, an Offering (provided, that this does not prevent Customer from comparing the Products to other products for Customer's Internal Use); (x) use any feature of ARIA Cybersecurity APIs for any purpose other than in the performance of, and in accordance with, this Agreement; or (xi) cause, encourage or assist any third party to do any of the foregoing. Customer agrees to use an Offering in accordance with laws, rules and regulations directly applicable to Customer and acknowledges that Customer is solely responsible for determining whether a particular use of an Offering is compliant with such laws.

3.4 Installation and User Accounts. ARIA Cybersecurity is not responsible for installing Products unless Customer purchases installation services from ARIA Cybersecurity. For those Products requiring user accounts, only the single individual user assigned to a user account may access or use the Product. Customer is liable and responsible for all actions and omissions occurring under Customer's and its Customer Contractor's user accounts for Offerings. Customer shall notify ARIA Cybersecurity if it learns of any unauthorized access or use of Customer's user accounts or passwords for an Offering.

3.5 Malware Samples. If ARIA Cybersecurity makes malware samples available to Customer in connection with an evaluation or use of the Product ("Malware Samples"), Customer acknowledges and agrees that: (i) Customer's access to and use of Malware Samples is at Customer's own risk, and (ii) Customer should not download or have access any Malware Samples on or through its own production systems and networks and that doing so can infect and damage Customer's systems, networks, and data. Customer shall use the Malware Samples solely for Internal Use (on separately networked non-production systems) and not for any malicious or unlawful purpose. ARIA Cybersecurity will not be liable for any financial loss or damage caused by any Malware Sample regarless of the source, that may infect Customer's computer equipment, computer programs, data, or other proprietary material due to Customer's access to or use of the Malware Samples.

3.6 Ownership & Feedback. Products, Product-Related Services and the ARIA Cybersecurity Tools are made available for use or licensed, not sold. ARIA Cybersecurity owns and retains all right, title and interest (including all intellectual property rights) in and to the Products, Product-Related Services and the ARIA Cybersecurity Tools, excluding Customer Data. Any feedback or suggestions that Customer provides to ARIA Cybersecurity regarding its Offerings and ARIA Cybersecurity Tools (e.g., bug fixes and features requests) that is non-confidential, may be used by ARIA Cybersecurity for any purpose without acknowledgement or compensation; provided, Customer will not be identified publicly as the source of the feedback or suggestion.

4. Customer Contractors.

4.1 Authorization. Customer authorizes ARIA Cybersecurity to give Customer Contractors the rights and privileges to the Offerings necessary to enable and provide for Customer's use and receipt of the Customer Contractor Services. If at any time Customer revokes this authorization, to the extent the Offerings provide for Customer to limit the Customer Contractor's access and use of the Offerings, then Customer is responsible for taking the actions necessary to revoke such access and use. In the event Customer requires ARIA Cybersecurity assistance with such revocation or limitation, Customer must contact ARIA Cybersecurity Support with written notice of such revocation or limitation at support@ariacybersecurity.com and ARIA Cybersecurity will disable the Customer Contractor's access to Customer's Offerings within a reasonable period of time following receipt of such notice but in any event within 72 hours of receipt of such notice.

4.2 Disclaimer. Customer Contractors are subject to the terms and conditions in the Agreement while they are using the Offerings on behalf of Customer and Customer remains responsible for their acts and omissions during such time. Any breach by a Customer Contractor of this Agreement is a breach by Customer. ARIA Cybersecurity may make available Customer Contractor Services to Customer, for example, through an online directory, catalog, store, or marketplace. Customer Contractor Services are not required for use of the Offerings. Offerings may contain features, including API's, designed to interface with or provide data to Customer Contractor Services. ARIA Cybersecurity is not responsible or liable for any loss, costs or damages arising out of Customer Contractor's actions or inactions in any manner, including but not limited to, for any disclosure, transfer, modification or deletion of Customer Data (defined in Exhibit A). Whether or not a Customer Contractor is designated by ARIA Cybersecurity as, or otherwise claims to be "certified," "authorized," or similarly labeled, ARIA Cybersecurity does not: (i) control, monitor, maintain or provide support for, Customer Contractor Services, (ii) disclaims all warranties of any kind, indemnities, obligations, and other liabilities in connection with the Customer Contractor Services.

4.3 Restrictions on Customer Contractors. Customer shall not give or allow Customer Contractors access to, or use of, intelligence reports provided by, or made accessible in, the Products. For the avoidance of doubt, nothing herein prevents Customer from using intelligence API's in Customer Contractor Services for Customer's Internal Use.

5. Confidentiality.

5.1 Definitions. In connection with this Agreement, each party ("Recipient") may receive Confidential Information of the other party ("Discloser") or third parties to whom Discloser has a duty of confidentiality. "Confidential Information" means non-public information in any form that is in the Recipient's possession that the Discloser designates as confidential to Recipient or should be reasonably known by the Recipient to be Confidential Information. Confidential Information shall not include information that is: (i) in or becomes part of the public domain (other than by disclosure by Recipient in violation of this Agreement); (ii) previously known to Recipient without an obligation of confidentiality and demonstrable by the Recipient; (iii) independently developed by Recipient without use of Discloser's Confidential Information; or (iv) rightfully obtained by Recipient from third parties without an obligation of confidentiality.

5.2 Restrictions on Use. Recipient shall hold Discloser's Confidential Information in strict confidence and shall not disclose any such Confidential Information to any third party, other than to its employees, and contractors, (collectively, "Representatives"), its Affiliates and their Representatives, subject to the other terms of this Agreement, and in each case who need to know such information and who are bound by restrictions regarding disclosure and use of such information comparable to and no less restrictive than those set forth herein. Recipient shall not use Discloser's Confidential Information for any purpose other than as set forth in this Agreement. Recipient shall take the same degree of care that it uses to protect its own confidential information of a similar nature and importance (but in no event less than reasonable care) to protect the confidentiality of the Discloser's Confidential Information. If Recipient becomes aware of the unauthorized use, disclosure, publication, or dissemination of the Discloser's Confidential Information while in Recipient's control, Recipient shall promptly provide Discloser with notice thereof.

5.3 Exceptions. Recipient may disclose Discloser's Confidential Information: (i) to the extent required by applicable law or regulation; (ii) pursuant to a subpoena or order of a court or regulatory, self-regulatory, or legislative body of competent jurisdiction; (iii) in connection with any

regulatory report, audit, or inquiry; or (iv) where requested by a regulator with jurisdiction over Recipient. In the event of such a requirement or request, Recipient shall, to the extent legally permitted: (a) give Discloser prompt written notice of such requirement or request prior to such disclosure; and (b) at Discloser's cost, a reasonable opportunity to review and comment upon the disclosure and request confidential treatment or a protective order pertaining thereto prior to Recipient making such disclosure. If the Recipient is legally required to disclose the Discloser's Confidential Information as part of: (x) a legal proceeding to which the Discloser is a party but the Recipient is not; or (y) a government or regulatory investigation of the Discloser, the Discloser shall pay all of the Recipient's reasonable and actual out of pocket legal fees and expenses (as evidenced by reasonably detailed invoices) and will reimburse the Recipient for its reasonable costs and fees of compiling and providing such Confidential Information, including, a reasonable hourly rate for time spent preparing for, and participating in, depositions and other testimony.

5.4 Destruction. Upon Discloser's written request, Recipient shall use commercially reasonable efforts to destroy the Confidential Information and any copies or extracts thereof. However, Recipient, its Affiliates and their Representatives may retain any Confidential Information that: (i) they are required to keep for compliance purposes under a document retention policy or as required by applicable law, professional standards, a court, or regulatory agency; or (ii) have been created electronically pursuant to automatic or ordinary course archiving, back-up, security, or disaster recovery systems or procedures; provided, however, that any such retained information shall remain subject to this Agreement. Upon Discloser's request, Recipient will provide Discloser with written confirmation of destruction in compliance with this provision.

5.5 Equitable Relief. Each party acknowledges that a breach of this Section 7 (Confidentiality) shall cause the other party irreparable injury and damage. Therefore, each party agrees that those breaches may be stopped through injunctive proceedings in addition to any other rights and remedies which may be available to the injured party at law or in equity without the posting of a bond.

6. Warranties & Disclaimer.

6.1 No Warranty for Pre-Production Versions. Any pre-production feature or version of an Offering provided to Customer is experimental and provided "AS IS" without warranty of any kind and will not create any obligation for ARIA Cybersecurity to continue to develop, productize, support, repair, offer for sale, or in any other way continue to provide or develop any such feature or Offering.

6.2 Product Warranty. If Customer has purchased a Product, ARIA Cybersecurity warrants to Customer during the applicable Subscription/Order Term that: (i) the Product will operate in material conformance with the Documentation; and (ii) ARIA Cybersecurity has used industry standard techniques to prevent the Products at the time of delivery from injecting malicious software viruses into your Endpoints where the Products are installed. You must notify ARIA Cybersecurity of any warranty claim during the Subscription/Order Term. Your sole and exclusive remedy and the entire liability of ARIA Cybersecurity for its breach of this warranty will be for ARIA Cybersecurity, at its own expense to do at least one of the following: (a) use commercially reasonable efforts to provide a work-around or correct such Error; or (b) terminate your license to access and use the applicable non-conforming Product and refund the prepaid fee prorated for the unused period of the Subscription/Order Term. ARIA Cybersecurity shall have no obligation regarding Errors reported after the applicable Subscription/Order Term.

6.3 Professional Services Warranty. ARIA Cybersecurity warrants to you that it will perform all purchased Professional Services in a professional and workmanlike manner consistent with generally accepted industry standards. You must notify ARIA Cybersecurity of any warranty claim for Services during the period the Services are being performed or within 30 days after the conclusion of the Services. Your sole and exclusive remedy and the entire liability of ARIA Cybersecurity for its breach of this warranty will be for ARIA Cybersecurity, at its option and expense, to (a) use commercially reasonable efforts to re-perform the non-conforming Services, or (b) refund the portion of the fees paid attributable to the non-conforming Services.

6.4 General Warranty. ARIA Cybersecuirty warrants that: (i) it has full power and authority to enter into this Agreement and to perform its obligations hereunder; (ii) ARIA Cybersecurity has obtained or will obtain all licenses or similar rights required by any third party to provide Customer the full use and benefit of the Products and Services under this Agreement; (iii) there are no consents or authorizations of any individuals or entities required in connection with the execution or performance of this Agreement; (iv) as of the Effective Date, ARIA Cybersecurity is not under investigation by the Federal Trade Commission, state attorneys general, or any similar regulatory agency or legislative body, or the subject of any pending litigation, disputes, or threats thereof relating to privacy or data security; (v) ARIA Cybersecurity does and will comply with all applicable laws; and (vi) the execution and performance of this Agreement does not and will not conflict with, breach or otherwise violate any other agreement or obligation to which ARIA Cybersecurity is bound.

6.5 Exclusions. The express warranties do not apply if the applicable Product or Service: (i) has been modified, except as approved by or by ARIA Cybersecurity, (ii) has not been installed, used, or maintained in accordance with this Agreement or Documentation, or (iii) is non-conforming due to a failure to use an applicable Update, when such Update was provided at no cost to Customer. If any part of a Product or Service references websites, hypertext links, network addresses, or other third-party locations, information, or activities, it is provided as a convenience only.

6.6 NO GUARANTEE. CUSTOMER ACKNOWLEDGES, UNDERSTANDS, AND AGREES THAT ARIA CYBERSECURITY DOES NOT GUARANTEE OR WARRANT THAT IT WILL FIND, LOCATE, OR DISCOVER ALL OF CUSTOMER'S OR ITS AFFILIATES' SYSTEM THREATS, VULNERABILITIES, MALWARE, AND MALICIOUS SOFTWARE, AND CUSTOMER AND ITS AFFILIATES WILL NOT HOLD ARIA CYBERSECURITY RESPONSIBLE THEREFOR.

6.7 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES IN THIS SECTION 8, ARIA CYBERSECURITY AND ITS AFFILIATES DISCLAIM ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, ARIA CYBERSECURITY AND ITS AFFILIATES AND SUPPLIERS SPECIFICALLY DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT THERE IS NO WARRANTY THAT THE OFFERINGS OR ARIA CYBERSECURITY TOOLS WILL BE ERROR FREE, PERFROMANCE FAIL-SAFE OR THAT THEY WILL OPERATE WITHOUT INTERRUPTION OR WILL FULFILL ANY OF CUSTOMER'S PARTICULAR PURPOSES OR NEEDS. Customer agrees that it is Customer's responsibility to ensure safe use of an Offering and the ARIA Cybersecurity Tools in such applications and installations. ARIA CYBERSECURITY DOES NOT WARRANT ANY THIRD-PARTY PRODUCTS OR SERVICES.

6.8 Additional Terms: Additional terms may apply for any statement of work (SoW) specified requirements for ARIA products and services. Those terms will accompany those statements of work. Such terms and conditions are additional to and do not alter nor diminish these standard terms and conditions as specified here.

7. Compliance with Laws. Each party agrees to comply with all U.S. federal, state, local and non-U.S. laws directly applicable to such party in the performance of this Agreement, including but not limited to, applicable export and import, anti-corruption and employment laws. Customer acknowledges and agrees the Offerings shall not be used, transferred, or otherwise exported or re-exported to regions that the United States maintains an embargo or comprehensive sanctions (collectively, "Embargoed Countries"), or to or by a national or resident thereof, or any person or entity subject to individual prohibitions (e.g., parties listed on the U.S. Department of Treasury's List of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders) (collectively, "Designated Nationals"), without first obtaining all required authorizations from the U.S. government and any other applicable government. Customer represents and warrants that Customer is not located in, or is under the control of, or a national or resident of, an Embargoed Country or Designated National. ARIA Cybersecurity represents and warrants that ARIA Cybersecurity is not located in, or is under the control of, or a national or resident of, an Embargoed Country or Designated National.

8. Customer Obligations. Customer, along with its Affiliates, represents and warrants that: (i) it owns or has a right of use from a third party, and controls, directly or indirectly, all of the software, hardware and computer systems (collectively, "Systems") where the Products and/or ARIA Cybersecurity Tools will be installed or that will be the subject of, or investigated during, the Offerings, (ii) to the extent required under any federal, state, or local U.S. or non-US laws (e.g., Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq., Title III, 18 U.S.C. 2510 et seq., and the Electronic Communications Privacy Act, 18 U.S.C. § 2701 et seq.) it has authorized ARIA Cybersecurity to access the Systems and process and transmit data through the Offerings and ARIA Cybersecurity Tools in accordance with this Agreement and as necessary to provide and perform the Offerings, (iii) it has a lawful basis in having ARIA Cybersecurity investigate the Systems, process the Customer Data and the Personal Data; (iv) that it is and will at all relevant times remain duly and effectively authorized to instruct ARIA Cybersecurity to carry out the Offerings, and (v) it has made all necessary disclosures, obtained all necessary consents and government authorizations required under applicable law to permit the processing and international transfer of Customer Data and Customer Personal Data from each Customer and Customer Affiliate, to ARIA Cybersecurity.

9. Suspension and Termination. This Agreement shall remain effective until termination in accordance with this Section or as otherwise specified herein. ARIA Cybersecurity may immediately suspend Customer's access to, or use of, the Offerings if: (i) ARIA Cybersecurity believes that there is a significant threat to the security, integrity, functionality, or availability of the Offerings or any content, data, or applications in the Offerings; (ii) Customer or Customer users are in breach of Section 3.3 (Restrictions); or (iii) Customer fails to pay ARIA Cybersecurity when undisputed fees are due; provided, however, ARIA Cybersecurity will use commercially reasonable efforts under the circumstances to provide Customer with notice and, if applicable, an opportunity to remedy such violation prior to any such suspension. Either party may terminate this Agreement upon 30 days' written notice of a material breach by the other party, unless the breach is cured within the 30-day notice period. In the event this Agreement is terminated due to ARIA Cybersecurity's breach, Customer shall receive a refund the pre-paid, unused fees paid by Customer

corresponding to the unused period of the Subscription/Order Term. Prior to termination and subject to the terms of this Agreement, Customer shall have the right to access and download Customer Data available per the Customer's purchased Products and data retention period in a manner and in a format supported by the Products. Upon termination of this Agreement for any reason: (a) all Customer's access and use rights granted in this Agreement will terminate; (b) Customer must promptly cease all use of Offerings and de-install all Software Components installed on Customer's Endpoints; and (c) Customer Data will be deleted in accordance with the data retention period purchased by Customer and Section 5.4 Confidentiality; Destruction). Sections 1, 3.3, 7, 10, 12, 13, and 14 and all liabilities that accrue prior to termination shall survive expiration or termination of this Agreement for any reason.

10. General.

10.1 Entire Agreement. This Agreement, including Exhibit A hereto, constitutes the entire agreement between Customer and ARIA Cybersecurity concerning the subject matter of this Agreement and it supersedes all prior and simultaneous proposals, agreements, understandings, or other communications between the parties, oral or written, regarding such subject matter. Notwithstanding the foregoing, if you have a ARIA Cybersecurity Limited Warranty Agreement for Myricom products (or a preceding or successor named product) fully executed with ARIA Cybersecurity, the warranty provided therein stands alone and is not superseded by this Agreement. It is expressly agreed that the terms of this Agreement shall supersede any terms in any procurement Internet portal or other similar non-ARIA Cybersecurity document and no such terms included in any such portal or other non-ARIA Cybersecurity document shall apply to the Offerings ordered. Any Order through a reseller is subject to, and ARIA Cybersecurity's obligations and liabilities to Customer are governed by, this Agreement. ARIA Cybersecurity is not obligated under any reseller's agreement with Customer. This Agreement shall not be construed for or against any party to this Agreement because that party or that party's legal representative drafted any of its provisions.

10.2 Assignment. Neither party may assign this Agreement without the prior written consent of the other party, except to an Affiliate in connection with a corporate reorganization or in connection with a merger, acquisition, or sale of all or substantially all of its business and/or assets. Any assignment in violation of this Section shall be void. Subject to the foregoing, all rights and obligations of the parties under this Agreement shall be binding upon and inure to the benefit of and be enforceable by and against the successors and permitted assigns.

10.3 Governing Law; Venue. THIS AGREEMENT IS GOVERNED BY AND SHALL BE CONSTRUED IN ACCORDANCE WITH LAWS OF THE STATE OF MASSACHUSETTS WITHOUT GIVING EFFECT TO ANY CHOICE OR CONFLICT OF LAW PROVISION OR RULE (WHETHER OF THE STATE OF NEW YORK OR ANY OTHER JURISDICTION) THAT WOULD CAUSE THE APPLICATION OF THE LAWS OF ANY JURISDICTION OTHER THAN THE STATE OF NEW YORK. THE PARTIES MUTUALLY CONSENT TO THE JURISDICTION OF THE US FEDERAL AND STATE COURTS IN BOSTON MASSACHUSETTS

10.5 Independent Contractors; No Third-Party Rights. The parties are independent contractors. This Agreement shall not establish any relationship of partnership, joint venture, employment, franchise, or agency between the parties. No provision in this Agreement is intended or shall create any rights with respect to the subject matter of this Agreement in any third party.

10.6 Waiver, Severability & Amendments. The failure of either party to enforce any provision of this Agreement shall not constitute a waiver of any other provision or any subsequent breach. If any provision of this Agreement is held to be illegal, invalid, or unenforceable, the provision will be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remaining provisions of this Agreement will remain in full force and effect. This Agreement may only be amended, or any term or condition set forth herein waived, by written consent of both parties.

10.7 Force Majeure. Neither party shall be liable for, nor shall either party be considered in breach of this Agreement due to, any failure to perform its obligations under this Agreement (other than its payment obligations) as a result of a cause beyond its control, including but not limited to, act of God or a public enemy, act of any military, civil or regulatory authority, change in any law or regulation, fire, flood, earthquake, storm or other like event, disruption or outage of communications (including an upstream server block and Internet or other networked environment disruption or outage), power or other utility, labor problem, or any other cause, whether similar or dissimilar to any of the foregoing, which could not have been prevented with reasonable care. The party experiencing a force majeure event, shall use commercially reasonable efforts to provide notice of such to the other party.

10.8 Notices. All legal notices will be given in writing to the addresses in the Purchase Order or Order confirmations and will be effective: (i) when personally delivered, (ii) on the reported delivery date if sent by a recognized international or overnight courier, or (iii) five business days after being sent by registered or certified mail (or ten days for international mail) , or (iv) on the reported delivery date if sent by email. For clarity, Orders, POs, confirmations, invoices, and other documents relating to order processing and payment are not legal notices and may be delivered electronically in accordance with each party’s standard ordering procedures.