ARMIS PLATFORM TERMS AND CONDITIONS

These Armis Platform Terms and Conditions (these "**Terms**") are between the Armis entity identified in Section 16.1 below ("**Armis**") and the customer who purchased the subscription to the Armis Solutions ("**Customer**"). Armis and Customer may be referred to individually as a "**Party**" or collectively as the "**Parties**." Capitalized terms used in these Terms have the meanings assigned to such terms as designated herein. Unless Customer and Armis have signed another agreement which expressly governs Customer's subscription to and use of the Armis Solutions and overrides these Terms, by accepting these Terms via the signing or otherwise indicating acceptance of an applicable Purchase Order, (and such date, the Effective Date unless another date is indicated in the Purchase Order as described in Section 4.1), Customer agrees to be bound by these Terms and the person acting on Customer's behalf hereby represents to Armis that they have the authority to bind Customer to these Terms through such consent or access to the Armis Solutions. If Customer does not agree to these Terms or you do not have the authority to bind Customer to these Terms, then Customer may not access or use the Armis Solutions. The Parties agree as follows:

1. Definitions.

1.1. "**Affiliate**" means any entity that directly, or indirectly through intermediaries, is controlled by, or is under common control with a Party.

1.2. "**Armis APIs**" means the Armis' proprietary application programming interfaces and/or software development kits (SDK) made available to Customer for use in integrating the Armis Platform with other products and applications, in each case solely in accordance with the Armis API/SDK License Agreement available here: https://www.armis.com/legal-compliance/.

1.3. "**Armis Assets**" means: (i) the Armis Solutions and Documentation; and (ii) all specifications, technology, software (including all underlying source code and object code), data, methodologies, machine learning models, user interfaces, algorithms, enhancements, components, documentation, techniques, designs, inventions, works of authorship, and know-how, in each case, that are used to provide, or made available in connection with, any of the Armis Solutions, and in each case all associated Intellectual Property Rights, and any subsequent updates, upgrades, and derivatives of any of the foregoing.

1.4. "**Armis On-Prem Module(s)**" means either Armis Centrix© for OT/IoT Security On Prem, Armis Centrix for Secure Remote Access, or both, as ordered by Customer. The Armis On-Prem Modules provide Armis Centrix© functionality and/or secure remote access functionality via a copy of such Armis Platform module(s) locally downloaded and operating within Customer's hardware environment.

1.5. "**Armis Platform**" means (i) the Armis Software as a Service (SaaS) modules; (ii) Collectors; (iii) Collector Technology; and (iv) any other Armis Platform modules provided under an Armis Platform Addendum to these Terms.

1.6. "**Armis Platform Addendum**" means any of the Addendums referenced in Section 2.2, below.

1.7. "**Armis Solutions**" means: (i) the Armis Platform; (ii) Armis APIs; and (iii) Professional Services.

1.8. "**Authorized User**" means any individual who accesses or uses the Armis Solutions on behalf of Customer or its Affiliates.

1.9. "**Collector**" means hardware, if any, such as servers or network ports, provided by or on behalf of Armis to Customer to enable the use of the Armis Platform.

1.10. "**Collector Technology**" means Armis' virtual machine images or Collector-related software provided by or on behalf of Armis to Customer to enable use of the Armis Platform.

1.11. "**Customer Data**" means Customer's network, connected devices, code and/or other data automatically collected, processed, and hosted by the Armis Platform through Customer's use of the Armis Solutions, including copies, modifications, and other derivatives of such data that is generated by the Armis Platform through Customer's use of the Armis Platform. Customer Data does not include Statistical Data.

1.12. "**Documentation**" means any technical user guides, manuals, release notes, installation notes, specifications, "read-me" files, support guides, and other materials related to the Armis Solutions, and the use, operation, and maintenance thereof, including all enhancements, modifications, derivative works, and amendments to the same, in each case, that Armis publishes or provides to Customer through its Support Portal available at: https://support.armis.com/s/login (or any

successor website, "**Support Portal**").

1.13. "**Intellectual Property Rights**" means all patents, copyrights, moral rights, trademarks, trade secrets, and any other form of intellectual property rights recognized in any jurisdiction, including applications and registrations for any of the foregoing.

1.14. "**Laws**" means, collectively, any laws, statutes, ordinances, regulations and other types of government authority, promulgated under such authority anywhere in the world.

1.15. "**Partner**" means an authorized Armis partner, including a reseller, marketplace, or implementation partner.

1.16. "**Purchase Order**" means: (i) an order form (including a Quote) executed by Armis and Customer; or (ii) a purchase order, statement of work, or other similar document issued by Customer or a Partner in each case solely to the extent its terms match and do not deviate from a corresponding Quote (and in the event of a conflict between a Purchase Order and a Quote, the Purchase Order shall only be valid to the extent it matches and does not deviate from the applicable Quote). If Customer orders Armis Solutions through a Partner or marketplace, then such Partner's or marketplace's applicable ordering document will apply solely with respect to the fees payable by Customer, volumes, and Subscription Term of Armis Solutions ordered.

1.17. "**Quote**" means a quote prepared and issued by Armis to Customer or a Partner that forms part of these Terms and describes the Armis Solutions ordered by Customer and any associated terms and fees.

1.18. "**Professional Services**" means any services (beyond the Armis support provided pursuant to Section 2.4.1) such as advisory, consulting, implementation, integration, or training services, that may be provided by or on behalf of Armis to Customer as detailed in an applicable Purchase Order.

1.19. "**Statistical Data**" means data generated in relation to Customer's use of the Armis Platform that has been irreversibly anonymized as to Customer and aggregated by Armis, including generic device descriptions and performance metadata about devices that appear in Customer's instance of the Armis Platform, such as the device manufacturer, type of operating system, and device model. Statistical Data does not include: (i) any identifiers that would link any devices to Customer, such as IP addresses, MAC addresses, or unique Customer identifiers; or (ii) any other data processed on or hosted by any Customer device.

2. Armis Platform.

2.1. **Access and Use.** During the Subscription Term and subject to Customer's compliance with these Terms, Armis grants Customer a subscription to access and use the Armis Platform in accordance with the Documentation, solely for Customer's internal business purposes, and subject to any use limitations indicated in the applicable Purchase Order. The rights granted to Customer herein include the right to deploy and use the Armis Platform at Customer's Affiliates' environments, provided Customer remains fully responsible and liable under these Terms for Customer's Affiliates' use. In addition to any access rights a Customer Affiliate may have as aforesaid, a Customer Affiliate may separately subscribe to Armis Solutions pursuant to these Terms by entering into a Purchase Order, and in each case, all references in these Terms to Customer will be deemed to refer to the applicable Affiliate for purposes of that Purchase Order.

2.2. **Additional Armis Products.** Customer may subscribe to one or more Armis On-Prem Modules or Armis Data Products ("**Additional Armis Products**") as detailed in an applicable Purchase Order. Armis shall provide Customer such Additional Armis Products subject to an Armis Platform Addendum that Customer accepts by clicking through to access the Additional Armis Products, or by otherwise indicating Customer's acceptance of such Armis Platform Addendum through access to and/or use of the Additional Armis Products. Armis On-Prem Modules are subject to an Armis On-Prem Subscription Addendum and Armis Data Products are subject to an Intelligence Center and Early Warning Addendum attached hereto, unless Customer and Armis have signed another agreement or addendum which expressly governs Customer's subscription to and use of the Additional Armis Products and overrides the Armis Platform Addendum.

2.3. **Customer Responsibilities**. The Armis Platform may be used by or for Customer only through an account that is specific to Customer and only by Authorized Users. Customer is solely responsible for: (i) identifying and authenticating all Authorized Users, approving access by such Authorized Users to the Armis Platform, and ensuring each Authorized User complies with these Terms; (ii) ensuring that Authorized Users keep their login credentials safe and secure; (iii) all activities that occur under the login credentials of Authorized Users; and (iv) the accuracy, quality, and legality of Customer Data, the means by which Customer acquired Customer Data, Customer's use of Customer Data with the Armis Platform, and the interoperation of any Non-Armis Products with which Customer uses the Armis Platform. Armis is not responsible for any losses or damages arising due to any breach of these Terms by any Authorized User or any other personnel, agent, or

advisor of Customer. Customer shall notify Armis immediately upon becoming aware of any unauthorized access to or use of the Armis Platform.

2.4. **Provision of the Armis Solutions.**

2.4.1. **Support**. Armis shall provide Customer with standard support (at no additional cost) unless Customer purchases upgraded support as set forth in a Purchase Order. Armis shall provide the technical support and service level commitments set forth in Armis' Platform Support Terms ("**SLA**"), as non-materially updated from time to time, available in the Support Portal. Except for critical updates, Armis schedules maintenance during non-peak usage hours (that reasonably minimizes the impact on all customers worldwide) and shall provide reasonable advance notice through the Armis Platform of any planned downtime in accordance with the SLA.

2.4.2. **Updates**. Armis makes updates (e.g., bug fixes, enhancements) to the Armis Platform on an ongoing basis, which are delivered through the Armis Platform. Customer's subscription includes all updates that Armis makes generally available to its customers at no additional charge. To the extent Customer's configuration of the Armis Platform requires acceptance of updates, Customer shall accept such updates in a timely manner. Armis is not responsible for the proper performance of the Armis Platform or for any security issues encountered with the Armis Platform resulting from any delay or failure to accept such updates. Armis may update the content, functionality, and user interface of the Armis Platform from time to time, provided that such update will not materially decrease the functionality of the Armis Platform during the Subscription Term. Customer's use of the Armis Solutions under these Terms is not contingent on the delivery of any future features or functionality.

2.4.3. **Subcontractors**. Armis may utilize subcontractors in the provision of the Armis Solutions, including to process Customer Data, provided that such subcontractors: (i) are subject to confidentiality obligations materially as protective of Customer Data as those set forth herein; and (ii) maintain commercially reasonable technical, physical, and organizational measures designed to protect the security, confidentiality, and integrity of Customer Data, taking into account the state of the art, costs of implementation, and the type of data. Armis will be liable for the acts and omissions of its subcontractors to the extent such acts or omissions constitute a breach of these Terms.

2.5. **Professional Services**. During the Subscription Term, Customer may receive Professional Services subject to these Terms as detailed in a Purchase Order. If applicable, the Armis Quote for Professional Services will identify any additional terms that apply with respect to such Professional Services.

2.6. **Data Protection and Security.** Armis shall implement and maintain commercially reasonable technical, physical, and organizational measures designed to protect the security, confidentiality, and integrity of Customer Data, taking into account the state of the art, costs of implementation, and the type of data, in accordance with Armis' information security program, as updated from time to time. Any updates to Armis' information security program will not materially diminish Armis' current data security obligations, a summary of which is available at: https://www.armis.com/legal-compliance/information-security-disclosure/ (or successor website). In addition, the terms and conditions of Armis' Data Processing Addendum ("**DPA**") attached hereto(or successor website), apply to the processing of any Personal Data (as defined in the DPA). Armis shall promptly notify Customer upon becoming aware of a breach of the aforementioned security measures within Armis' network leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data ("**Security Incident**"), and Armis shall reasonably cooperate with Customer in the investigation and mitigation thereof. Armis' obligation to report or respond to a Security Incident is not an acknowledgement by Armis of any fault or liability with respect to such Security Incident. In addition, Armis shall use commercially reasonable efforts to respond, once per year, to any reasonable written inquiries from Customer regarding compliance with this Section 2.6, including requests for Armis' most recent third-party auditor reports regarding Armis' information security program.

2.7. **Non-Armis Service Providers.** Customer may engage one or more third parties to manage the installation, onboarding, and/or operation of the Armis Platform on Customer's behalf ("**Non-Armis Service Provider**"), provided that Customer delivers written notice to Armis in advance of such engagement. Customer shall require the Non-Armis Service Provider to comply with these Terms and shall ensure that such Non-Armis Service Provider uses the Armis Platform solely on behalf of Customer. Customer will be fully liable for the acts and omissions of its Non-Armis Service Providers to the extent such acts or omissions constitute a breach of these Terms.

2.8. **Non-Armis Products.** Customer may from time to time decide to use an integration between Non-Armis Products and the Armis Platform. "**Non-Armis Products**" means third-party products, applications, services, software, networks, or other

systems or information sources acquired by Customer that are not developed by Armis or provided by Armis as part of the Armis Platform. Use of Non-Armis Products is subject to the end user license or other agreement between Customer and the provider of the Non-Armis Products. Armis has no liability with respect to the implementation, maintenance, use, or continued interoperability of any Non-Armis Products, even if Armis designates them as approved or recommended or is an authorized reseller of such Non-Armis Products. By enabling any interoperability between Non-Armis Products and the Armis Platform, Customer expressly agrees to the transfer of any Customer Data between Armis and the provider of the Non-Armis Product as required for such interoperability.

2.9. **Restrictions**. Customer and its Authorized Users shall not, and shall not authorize any third party to: (i) decompile, disassemble, reverse engineer, copy, frame, or mirror any part of the Armis Assets, or otherwise attempt to derive the source code, structure, ideas, algorithms, or associated know-how of any Armis Assets; (ii) translate, adapt, or modify any Armis Assets; (iii) write or develop any program based upon any Armis Assets, or otherwise access, test, or use any Armis Assets for the purpose of developing or distributing products or services that compete with any Armis Assets; (iv) sell, sublicense, transfer, assign, lease, rent, distribute, grant a security interest in, or otherwise commercially exploit any Armis Assets or make available to a third party any Armis Assets except as expressly authorized in these Terms; (v) use the Armis Assets other than as expressly permitted by these Terms and solely for Customer's internal business operations and in conformity with the Documentation; (vi) alter or remove any trademarks or proprietary notices contained in or on the Armis Assets; (vii) attempt to gain access to the Armis Platform or its related systems or networks through unauthorized means, including any automated means (i.e., use of scripts or web crawlers), circumvent or interfere with any authentication or security measures of the Armis Platform, or otherwise interfere with or disrupt the integrity or performance of the Armis Platform; (viii) probe, scan, or test the vulnerability of any Armis system or network; (ix) conduct any competitive analysis, publish or share with any third party any results of any technical evaluation or benchmark tests performed on Armis Assets, or disclose Armis Assets' features, errors, or bugs to a third party without Armis' prior written consent; or (x) use any portion of the Armis Assets in violation of any applicable Laws or transmit to or from the Armis Assets any data, materials, or other content that infringes, misappropriates, or otherwise violates any third-party rights. Customer shall promptly notify Armis in writing if it becomes aware of, or has reason to believe, that any of the prohibitions in this Section have been breached by Customer, its Affiliates or any Authorized User.

3. **Collectors**. The Armis Platform may include Collectors that are provided to Customer during the Subscription Term under an applicable Purchase Order. Customer shall use and reasonably maintain Collectors in good working order in accordance with the Documentation and at the locations agreed to by the Parties to enable proper usage and operation of the Armis Platform. Support for Collectors is provided pursuant to Armis' standard support services, as described in the SLA and in the Documentation, which may require installation of a current release of Collector Technology. Without Armis' express written permission, Customer shall not, and shall not permit any third party to: (i) use Collectors other than for the express purpose for which they were provided; (ii) rent or lease Collectors to any third party; (iii) transfer or copy the Collector Technology within the Collector to any other product or device; or (iv) install the Collector Technology on any device other than the applicable Collector for which it was provided. The Armis Platform may not operate as intended if Collectors are moved to any other geographic location without Armis' prior express written permission.

4. **Purchase Orders and Fees.**

4.1. **Subscription Term and Purchase Orders**. Each Purchase Order will commence on the subscription start date (the "**Effective Date**") stated in such Purchase Order and continue until the subscription end date stated therein ("**Subscription Term**"). Unless otherwise specified in a Purchase Order: (i) subscriptions for the Armis Solutions may be renewed for additional one (1) year terms by executing a written order for the successive annual term; (ii) discounts or other promotional pricing offered for the Armis Solutions are one-time and valid only for the specific amount purchased; (iii) renewal of any discounted Armis Solutions will be at Armis' applicable list price then in effect in accordance with the applicable GSA Schedule Pricelist, and any change in the amount of, or term for, the Armis Solutions may result in re-pricing without regard to prior pricing; and (iv) during a Subscription Term, any purchase of additional amounts will be priced at Armis' applicable list price then in effect.

4.2. **Fees**. For direct purchases from Armis, Customer shall pay Armis or its authorized reseller as applicable the fees and other amounts detailed in any applicable Purchase Order in accordance with the terms therein. If applicable, Customer shall reimburse Armis for reasonable, documented, out-of-pocket expenses (including all travel costs and expenses) that are authorized by Customer in writing and that are incurred by Armis in the course of providing Professional Services. If Customer's use of the Armis Solutions exceeds the usage limitations set forth in the applicable Purchase Order, then Armis may invoice Customer, and Customer shall pay, for such excess usage at Armis' then current rates, prorated for the remainder of the Subscription Term. Upon renewal, Customer's subscription will be increased to reflect Customer's actual usage during the preceding Subscription Term. Armis Solutions purchased cannot be decreased during a Subscription Term.

4.3. **Payment Terms**. Armis' obligations under these Terms are conditioned on Customer's payment in full of the fees when due as set forth in the applicable Purchase Order. For direct purchases from Armis, all fees are billed annually in U.S. Dollars with net thirty (30) payment terms from the start of the Subscription Term, unless alternate terms are stated in the applicable Purchase Order. Customer shall make any good faith dispute of an invoice in writing within thirty (30) days of the applicable invoice date. Any fees not paid when due or not subject to a good faith dispute will accrue interest on a daily basis until paid in full at the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid. Except as expressly stated in these Terms, all fees due or paid are non-cancellable and non-refundable. Neither Party may set-off fees payable under these Terms or a Purchase Order against any other amounts owed to such Party. Customer requirements for purchase orders, vendor registration forms, vendor portals, or the like, will not change Customer's payment obligations herein.

4.4. **Taxes**. Vendor shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k). These taxes (if applicable) will be stated separately on each invoice, unless Customer provides (in advance) a valid tax exemption certificate authorized by the applicable taxing authority.

5. **Beta Products**. FROM TIME TO TIME, ARMIS MAY OFFER CUSTOMER THE OPPORTUNITY (WHICH CUSTOMER MAY REFUSE IN ITS SOLE DISCRETION) TO USE EARLY AVAILABILITY OR BETA PRODUCTS, FEATURES, OR DOCUMENTATION (COLLECTIVELY, "**BETA PRODUCTS**"). BETA PRODUCTS MAY NOT BE GENERALLY AVAILABLE, ARE PROVIDED STRICTLY "AS IS," AND WILL NOT BE SUBJECT TO ANY REPRESENTATIONS, WARRANTIES, INDEMNIFICATION OBLIGATIONS, OR SUPPORT OBLIGATIONS. UNLESS PROHIBITED BY LAW, ARMIS WILL HAVE NO LIABILITY RELATED TO SUCH BETA PRODUCTS IN EXCESS OF ONE THOUSAND USD ($1,000.00 USD). CUSTOMER OR ARMIS MAY TERMINATE CUSTOMER'S ACCESS TO BETA PRODUCTS AT ANY TIME FOR ANY OR NO REASON.

6. **Ownership and Reservation of Rights.**

6.1. **Armis.** Except for the rights expressly granted to Customer in Section 2.1, as between the Parties, Armis and/or its licensors own and retain all rights, title, and interest, including Intellectual Property Rights, in and to all Armis Assets, Armis Confidential Information, and any other tangible and intangible material and information incorporated into or constituting any portion of the Armis Assets (excluding any Customer Data and Customer Confidential Information).

6.2. **Customer**. Except for the rights expressly granted to Armis in this Section 6, as between the Parties, Customer owns and retains all rights, title, and interest in and to Customer Data, Customer Confidential Information, and Feedback, including all associated Intellectual Property Rights. During the Subscription Term, Customer shall provide to Armis the right to access, process, transmit, store, use, and disclose Customer Data as necessary to provide the Armis Solutions to Customer and to improve the Armis Solutions including to identify, investigate, or resolve technical problems with the Armis Solutions.

6.3. **Feedback**. Customer or an Authorized User may provide to Armis, directly or indirectly, feedback, analysis, suggestions, or comments about the Armis Assets or Armis Solutions (collectively, "**Feedback**"). Feedback does not include Customer Data or Customer Confidential Information. Customer hereby grants to Armis a non-exclusive, perpetual, irrevocable, transferable, royalty-free, and worldwide right, with the right to grant and authorize sublicenses, to use and benefit from such Feedback to provide and improve the Armis Assets and Armis' business without any compensation or credit due to Customer to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

6.4. **Statistical Data**. During the Subscription Term, Armis may collect and compile Statistical Data and Armis owns and retains all rights, title, and interest in such Statistical Data. Armis may use Statistical Data for its own business purposes (such as improving, testing, and maintaining the Armis Solutions, including training Armis' machine learning algorithms and artificial intelligence models associated with the Armis Solutions, identifying trends, and developing additional products and services). For the avoidance of doubt, the use of Customer Data for the purpose of training Artificial Intelligence/Machine Learning (AI/ML) models and systems is prohibited without explicit written authorization from the Federal agency contracting officer.

6.5. **Reservation of Rights**. Each Party retains all rights that are not expressly licensed to the other Party in these Terms and does not grant the other Party any implied licenses in these Terms or under any other theory.

7. **Confidentiality.**

7.1. "**Confidential Information**" means any non-public information disclosed in any form or manner by one Party

("**Discloser**") to the other Party ("**Recipient**") that is marked as "confidential" or that Recipient knows or reasonably should know is confidential information of Discloser given the nature of such information and the circumstances of its disclosure. Confidential Information of Armis includes the Documentation, auditor reports, security test results and reports, and all communications related to updates to the Armis Assets. Confidential Information does not include Customer Data automatically uploaded to, processed, and hosted by the Armis Platform (the security and protection of which is governed by section 2.6), or any information which Recipient can demonstrate through reasonable evidence: (i) is or becomes generally known and available to the public through no act of Recipient; (ii) was already in Recipient's possession without a duty of confidentiality owed to Discloser at the time of receipt; (iii) is lawfully obtained by Recipient from a third party who has the express right to make such disclosure; or (iv) is independently developed by Recipient without breach of an obligation owed to Discloser.

7.2. During the Subscription Term, Recipient may use Discloser's Confidential Information solely for the purpose of performing its obligations under these Terms. Recipient shall use the same degree of care in protecting Discloser's Confidential Information as Recipient uses to protect its own Confidential Information from unauthorized use or disclosure, but in no event less than reasonable care. Recipient shall not disclose Discloser's Confidential Information to any third party except to its employees, consultants, affiliates, agents, and subcontractors having a need to know such Confidential Information to perform their respective obligations under these Terms and who are bound by a written undertaking of confidentiality that is at least as protective of Discloser's Confidential Information as set forth herein. In addition, Recipient may disclose Discloser's Confidential Information to the extent such disclosure is required by law or order of a court or similar judicial or administrative body, provided that Recipient notifies Discloser in advance (unless legally prohibited from doing so) to enable Discloser to seek a protective order or otherwise seek to prevent or restrict such disclosure. All right, title, and interest in and to Confidential Information is and will remain the sole and exclusive property of Discloser. Recipient is solely responsible and liable to Discloser for any act, omission, or other failure to comply with the Terms by any of its representatives. Armis recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

7.3. The use and disclosure restrictions in this Section 7 (Confidentiality) will survive the expiration or termination of these Terms for a period of three (3) years, provided that Confidential Information defined as a trade secret under any applicable Laws shall be maintained by Recipient in confidence so long as it retains trade secret status under such Laws.

8. **Warranties.**

8.1. **Armis Warranties.**

8.1.1. **Armis Platform Warranties.** Armis warrants that: (i) during the Subscription Term, the current versions of the Armis Platform will perform and function materially in accordance with the Documentation under normal and authorized use in compliance with these Terms; and (ii) Armis shall maintain appropriate technical measures and periodically update the Armis Platform to prevent the introduction of software viruses, disabling devices, trojans, worms, or other software or hardware devices designed to intentionally disrupt, disable, or harm Customer's network or systems or the operation of the Armis Platform. If Customer believes the Armis Platform does not conform to the warranties in this Section 8.1.1, Customer shall promptly notify Armis in writing (in no event later than thirty (30) days from the date of discovery of the nonconformity) by submitting a support ticket via the Support Portal in accordance with the SLA. In the event of a breach of the warranties in this Section 8.1.1, Armis' exclusive responsibility, and Customer's exclusive remedy (other than any termination rights Customer may have under Section 14), will be for Armis to either correct or replace, at no additional charge to Customer, the applicable deficiency in the Armis Platform in accordance with the SLA.

8.1.2. **Professional Services Warranty.** Armis warrants that, during the Subscription Term, the Professional Services will be performed in a workmanlike manner in accordance with current industry standards. If Customer believes the Professional Services do not conform to the warranty in this Section 8.1.2, Customer shall promptly notify Armis in writing (in no event later than thirty (30) days from the date the Professional Services were performed) by submitting a support ticket via the Support Portal in accordance with the SLA. Armis' exclusive responsibility, and Customer's exclusive remedy, will be for Armis, at its option and expense to: (i) re-perform the applicable Professional Services that fail to meet this warranty; or (ii) issue a refund of the fees paid for the applicable non-conforming Professional Services.

8.1.3. **Exceptions**. The warranties set forth in this Section 8.1 will not apply to the extent the nonconformity results from or is otherwise attributable to any failure or damage caused by the actions or inactions of Customer, Authorized Users, or any person acting at Customer's direction.

8.2. **Customer Warranty**. Customer warrants it will have all rights necessary, including any required consents, to provide or make available to Armis the Customer Data (including personal data) or other materials in connection with its use of the

Armis Solutions and to permit Armis to use Customer Data pursuant to these Terms.

9. **Mutual Representations**. Each Party represents that: (i) it is duly organized, validly existing and in good standing under the Laws of its jurisdiction of incorporation or organization; (ii) it has the full corporate power and authority to execute, deliver, and perform its obligations under these Terms; (iii) the person signing or clicking through these Terms on its behalf has been duly authorized and empowered to enter into these Terms; and (iv) these Terms are valid, binding, and enforceable against it in accordance with its terms.

10. **Compliance with Laws, Policies, and Trade Controls.**

10.1. In connection with the performance of these Terms each Party shall comply with all Laws applicable to such Party in the conduct of its business generally. In addition, if Customer's use of the Armis Solutions requires Customer to comply with industry specific Laws applicable to such use, Customer is responsible for such compliance.

10.2. Customer agrees that it will comply with all sanctions and export control Laws applicable to its activities carried out in connection with these Terms. Customer acknowledges and understands that Armis' products, software, and technology are (i) provided subject to compliance with U.S. sanctions and export control Laws, including but not limited to the U.S. Export Administration Regulations (EAR) and trade and economic sanctions maintained by the U.S. Office of Foreign Assets Control (OFAC), and (ii) may be subject to similar Laws of other countries (all of the foregoing, collectively, "**Trade Controls**").

10.2.1. Customer shall not directly or indirectly:(i) sell, export, reexport, transfer, divert, or otherwise dispose of any Armis' Asset(s) provided under these Terms to any entity, to (or in) any destination or person or (ii) or use such Armis Asset(s) in each case for any use prohibited by Trade Controls without first obtaining prior documented authorization from the competent government authority as required by Trade Controls. Prohibited end-uses include: restricted military, advanced computing, semiconductor manufacturing, supercomputing, nuclear, rocket systems and unmanned aerial vehicles, or chemical and biological weapons end-uses, in each instance as applicable under Trade Controls.

10.2.2. In addition, Customer shall not directly or indirectly sell, export, reexport, transfer, divert, or otherwise dispose of any Armis Asset(s) provided under these Terms: (i) to or in any country subject to an embargo or comprehensive Trade Controls by the U.S., EU, UN Security Council, or other applicable jurisdiction ("**Prohibited Country**"), or (ii) to any person or entity subject to individual (or entity) any prohibition or sanction, including, but not limited to, those listed on, or those majority-owned or controlled by anyone listed on, the U.S. Department of the Treasury's Specially Designated Nationals and Blocked Persons List, the U.S. Commerce Department's Denied Persons List, Entity List, Unverified List, or Military End-User List (each such person, a "**Designated National**"), in each case without first obtaining any required and documented authorization from the applicable government authority.

10.2.3. Customer represents and warrants that it is not, and it is not majority-owned or controlled by anyone who is, and is not not using and will not use any Armis Asset(s) on behalf of individual or entity who is (i) located in a Prohibited Country, or (ii) a Designated National. Customer agrees to cooperate promptly with any request by Armis for documentation relating to the above matters and to immediately inform Armis if it or anyone involved under these Terms becomes a Designated National.

11. **DISCLAIMER**. TO THE EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES SET FORTH ABOVE IN SECTIONS 8 (WARRANTIES), 9 (MUTUAL REPRESENTATIONS), AND 10 (COMPLIANCE WITH LAWS), NEITHER PARTY MAKES ANY, AND EACH PARTY HEREBY EXPRESSLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, WHETHER WRITTEN, ORAL, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, NON-INTERFERENCE, ACCURACY, CONDITION, AND FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITING THE FOREGOING, ARMIS MAKES NO REPRESENTATION OR WARRANTY: (I) AS TO ANY NON-ARMIS PRODUCT, EVEN IF SUCH NON-ARMIS PRODUCT INTEROPERATES WITH THE ARMIS SOLUTIONS; (II) THAT CUSTOMER'S USE OF THE ARMIS SOLUTIONS WILL BE UNINTERRUPTED, ERROR-FREE, OR HAVING NO NETWORK OR SYSTEM INTERRUPTION ASSOCIATED THEREWITH; OR (III) THAT THE ARMIS SOLUTIONS WILL DETECT, PREVENT, OR PROTECT AGAINST ALL POSSIBLE THREATS, VULNERABILITIES OR OTHER RISKS, WHETHER KNOWN OR UNKNOWN.

12. **Indemnification.**

12.1. **Armis**. Subject to the conditions of Section 12.3, Armis shall have the right to intervene to defend Customer against any claims, suits, actions, or proceedings brought against Customer and/or its directors, officers, and employees by a third party (including any regulatory authority) to the extent such claim alleges that Customer's permitted use of the Armis Solutions

under these Terms infringes or misappropriates the Intellectual Property Rights of a third party ("**IP Claim**"). Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. Armis shall indemnify Customer for all damages, fines, judgments, costs, and expenses, including reasonable attorneys' fees, that are finally awarded by a court of competent jurisdiction or that are agreed to by Armis in a monetary settlement in connection with an IP Claim. If any IP Claim is brought or threatened, Armis may, at its sole option and expense: (i) procure for Customer the right to continue to use the Armis Solutions; (ii) modify or replace the relevant portion(s) of the Armis Solutions with a non-infringing alternative having substantially equivalent performance; or (iii) terminate the applicable Purchase Order as to the infringing portion(s) of the Armis Solutions and issue a prorated refund of any unused prepaid fees applicable to such terminated Armis Solutions for the remaining period of the Subscription Term as calculated from the effective date of the termination. Notwithstanding the foregoing, Armis is not obligated to indemnify or defend any IP Claim to the extent arising from: (a) any use of the Armis Solutions in combination with software, products, or services not provided by Armis or any modification to the Armis Solutions by Customer or Authorized Users in each case not authorized by Armis, where the Armis Solutions would not be infringing but for such combination or modification; (b) Customer's failure to use the Armis Solutions in accordance with these Terms; or (c) the Customer Data.

12.2. **Reserved**.

12.3. **Procedures**. The Party seeking indemnification shall provide the indemnifying Party: (i) prompt written notice, provided that failure to provide such notice will not alleviate a Party's indemnification obligation to the extent any associated delay does not materially prejudice or impair the defense; (ii) sole control over the defense and settlement, provided that the indemnified Party's prior written approval will be required for any settlement that would reasonably be expected to impose an obligation on the indemnified Party; and (iii) all information and assistance reasonably requested by the indemnifying Party in connection with the defense or settlement, provided that the indemnifying Party shall reimburse the indemnified Party for any reasonable out-of-pocket costs of providing such assistance. This Section 12 states each Party's entire obligation and exclusive remedy regarding the third-party claims described in this Section 12.

13. **LIMITATION OF LIABILITY**. THE FOLLOWING TERMS APPLY TO THE EXTENT PERMITTED UNDER APPLICABLE LAW:

13.1. EACH PARTY'S TOTAL LIABILITY ARISING OUT OF OR RELATING TO THESE TERMS, WHETHER IN CONTRACT, TORT, OR ANY OTHER THEORY OF LIABILITY, WILL NOT EXCEED THE TOTAL AMOUNTS PAID OR PAYABLE BY CUSTOMER TO ARMIS OR AN ARMIS PARTNER IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE MOST RECENT EVENT GIVING RISE TO LIABILITY.

13.2. NOTWITHSTANDING SECTION 13.1 ABOVE, EACH PARTY'S TOTAL LIABILITY ARISING OUT OF OR RELATING TO ITS DATA SECURITY OR DATA PRIVACY OBLIGATIONS, WHETHER IN CONTRACT, TORT, OR ANY OTHER THEORY OF LIABILITY, WILL NOT EXCEED TWO (2) TIMES THE TOTAL AMOUNTS PAID OR PAYABLE BY CUSTOMER TO ARMIS OR AN ARMIS PARTNER IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE MOST RECENT EVENT GIVING RISE TO LIABILITY.

13.3. THE LIMITATIONS IN SECTIONS 13.1 AND 13.2 WILL NOT APPLY TO: (I) A PARTY'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 12 (INDEMNIFICATION); (II) LIABILITY FOR ANY INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS; (III) BREACH BY CUSTOMER OF SECTION 2.9 (RESTRICTIONS), BREACHES OF SECTION 7 (CONFIDENTIALITY); OR (IV) FEES FOR ARMIS SOLUTIONS OWED BY CUSTOMER UNDER THESE TERMS OR ANY PURCHASE ORDER.

13.4. IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR ANY THIRD PARTY FOR ANY LOSS OF PROFITS, LOSS OF USE, LOSS OF REVENUE, LOSS OF GOODWILL, ANY INTERRUPTION OF BUSINESS, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF OR RELATING TO THESE TERMS, WHETHER IN CONTRACT, TORT, OR ANY OTHER THEORY OF LIABILITY, EVEN IF SUCH DAMAGES WERE REASONABLY FORESEEABLE OR SUCH PARTY HAS BEEN ADVISED OR IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

13.5. THE LIMITATIONS OF LIABILITY, DISCLAIMERS OF REPRESENTATIONS AND WARRANTIES, AND EXCLUSION OF CERTAIN DAMAGES SET FORTH IN THESE TERMS REPRESENT A NEGOTIATED ALLOCATION OF RISK BETWEEN THE PARTIES (INCLUDING THE RISK THAT A REMEDY MAY FAIL OF

ITS ESSENTIAL PURPOSE) AND WILL BE GIVEN FULL EFFECT.

14. **Termination.**

14.1. **Right to Terminate**.When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Armis shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. If these Terms are terminated under Section 14.1, Armis shall issue a prorated refund of any unused prepaid fees for the remaining period of the Subscription Term as calculated from the effective date of the termination.

14.2. **Effect of Termination**. Upon termination or expiration of these Terms: (i) the access and usage rights granted in Section 2.1 will expire, and Armis will disable Customer's and each Authorized User's access to the Armis Solutions; (ii) Customer shall immediately and permanently delete all copies of the Documentation within its possession or control and Collector Technology installed on Customer's hardware devices; (iii) if Customer has Collectors: (a) Customer shall ensure that all Collectors remain connected to the internet for seven (7) days for Armis to permanently delete the Collector Technology; and (b) Customer shall return the Collectors to Armis in accordance with Armis' instructions; and (iv) Armis shall permanently delete all Customer Data in its possession or control sixty (60) days after termination or expiration in accordance with its automated deletion schedule. Prior to such deletion, Customer may export or download Customer Data at any time from the Armis Platform in accordance with the Documentation. Except as expressly set forth in these Terms or in a Purchase Order, any fees paid by Customer prior to the date of termination are non-refundable and Customer shall immediately pay Armis all fees owed but not yet paid. Any requested post-termination transition assistance is subject to mutual written agreement of the Parties.

14.3. **Suspension of Service**. Armis reserves the right to temporarily suspend Armis Solutions: (i) if Armis reasonably determines that Customer or its Authorized Users are in material breach of these Terms and such breach threatens the security, integrity, or availability of the Armis Solutions or any Armis systems; or (ii) if Armis reasonably determines that Customer or its Authorized Users are infringing or misappropriating Armis' Intellectual Property Rights. Depending on the severity of the violation, Armis may provide Customer's account administrator with notice and an opportunity to remedy such violation prior to suspension. Armis shall only suspend access to the extent reasonably necessary to address the violation and shall promptly restore access once the issue has been resolved.

15. **Insurance.** Armis shall, at its expense, procure and maintain commercially reasonable insurance coverage during the Subscription Term, including the following minimum policies and amounts: (i) Commercial General Liability Insurance: $1,000,000 per claim and $2,000,000 in the aggregate; (ii) Workers' Compensation and Employer's Liability Insurance: minimum amounts required by the state(s) in which work is to be performed, but not less than $1,000,000 each accident and $1,000,000 in the aggregate; (iii) Automobile Liability Insurance: combined single limit of $1,000,000 each accident; (iv) Umbrella or Excess Liability Insurance: $5,000,000 each claim and $5,000,000 in the aggregate; (v) Cyber Risk/E&O Insurance: $5,000,000 each claim and $5,000,000 in the aggregate. All of Armis' insurance policies will be underwritten by insurers that are rated "A-VII" or better. Upon Customer's written request, once per year during the Subscription Term, Armis shall provide a certificate of insurance evidencing its insurance coverage.

16. **General Provisions.**

16.1. **Parties, Governing Law, and Venue**. The Armis entity that Customer is contracting with under these Terms depends on where the Customer is domiciled as set forth below in this Section 16.1. These Terms are governed by and will be construed under the Federal Laws of the United States. The United Nations Convention on Contracts for the International Sale of Goods does not apply to these Terms or any Purchase Order.

16.1.1. If Customer is not domiciled in Europe, the Middle East, or Africa, the contracting entity is Armis, Inc., a Delaware corporation or, at Armis' election, Armis Federal, LLC, a Delaware limited liability company;

16.1.2. If Customer is domiciled in Europe, the Middle East (excluding Israel), or Africa, the Armis contracting entity is Armis Security UK Holdings Ltd., a United Kingdom limited company; or

16.1.3. If Customer is domiciled in Israel, the Armis contracting entity is Armis Security Ltd., an Israeli limited company.

16.2. **Reserved.**

16.3. **Notices**. The Parties shall provide all notices or communications related to these Terms via first-class mail (postage prepaid)

or email to the address designated in writing by such Party in these Terms or in the most recent Purchase Order. In case of notice to Armis, Customer shall send a copy of the notice to legal.notices@armis.com. Notice is effective on the earlier of five (5) days from being deposited for delivery or the date on the confirmed email or courier receipt. If an email address is not provided, Armis may use the administrator's contact information designated in the Armis Platform.

16.4. **Force Majeure**. In accordance with FAR Clause 52.212-4(f), Except for payment obligations, neither Party will be liable for any delay or failure to perform any of its obligations under these Terms resulting from circumstances beyond the reasonable control of such Party, including strikes, shortages, riots, insurrections, fires, floods, storms, explosions, acts of God, wars, actions by governmental or quasi-governmental authorities, acts of terrorism, earthquakes, power outages, internet or other technology failures, denial of service or similar attacks, or pandemics, epidemics, or similar regional health crises. Any dates by which performance obligations are scheduled to be met will be extended for a period equal to the time lost due to any force majeure event.

16.5. **Relationship of the Parties**. These Terms do not, and will not be construed to, create any relationship, partnership, joint venture, employer-employee, agency, or franchisor-franchisee relationship between the Parties. These Terms are personal to the Parties, and no third parties will be considered beneficiaries hereof for any purposes. The Parties shall not use the trademarks or service marks of the other Party without that Party's prior written consent, provided that Armis may name Customer as a user of the Armis Solutions.

16.6. **Assignment**. These Terms bind and benefit the Parties and the Parties' respective heirs, executors, administrators, legal representatives, and permitted successors and assigns. Neither Party may assign these Terms or any of its respective rights under these Terms, or delegate any of its obligations under these Terms (except for delegation by Armis to its subcontractors), without the prior written consent of the other Party, such consent not to be unreasonably withheld or delayed. Notwithstanding the foregoing, these Terms may be assigned by either Party in connection with a merger, consolidation, sale of all the equity interests of the Party, or a sale of all or substantially all the assets of the Party in accordance with the provisions set forth at FAR 42.1204. Any purported assignment of these Terms and rights herein or delegation of obligations in violation of this Section will be null and void and of no effect. Armis may disclose the relationship between it and Customer if legally required or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all its assets.

16.7. **Amendment and Waiver.** These Terms and any Purchase Order may not be amended or superseded except by written, executed agreement of the Parties that expressly identifies itself as an amendment or replacement of these Terms or any such Purchase Order. A written, executed agreement does not include: (i) the text of e-mails or similar electronic transmissions; (ii) the terms of any shrink-wrap, click-wrap, browse-wrap or similar agreement between the Parties; or (iii) the terms of any website owned, operated, or controlled by either Party or any of its affiliates or other service providers. Any waiver of these Terms must be in writing and no written waiver will operate or be construed as a waiver of any subsequent breach. Failure of a Party to enforce its rights on one occasion will not result in a waiver of such rights on any other occasion.

16.8. **Severability**. If any term of these Terms is found to be invalid or unenforceable, the remaining terms of these Terms will remain in full force and effect and the invalid or unenforceable provision will be deemed modified so that it is valid and enforceable to the maximum extent permitted by law.

16.9. **Survival**. Any terms that are expressly stated to survive or by their nature survive termination or expiration hereof will survive (including Sections 4 (Purchase Orders and Fees), 6 (Ownership and Reservation of Rights), 7 (Confidentiality), 12 (Indemnification), 13 (Limitation of Liability), 14 (Termination), and 16 (General Provisions)).

16.10. **Entire Agreement**. These Terms, together with all documents referred to herein (including by hyperlink) or attached hereto, constitute the final agreement between the Parties and are the complete and exclusive expression of the Parties' agreement on the matters contained herein. All prior and contemporaneous representations, responses to proposals, understandings, and agreements (written or verbal) relating to the matters herein (including any confidentiality or evaluation agreements previously entered into by the Parties still in effect) are expressly superseded by these Terms. In entering into these Terms, neither Party has relied on any statement, representation, warranty, or agreement of the other Party except for those expressly stated herein. After the Effective Date, Customer or a Partner may for its convenience provide Armis (including through a web portal) a purchase order, vendor onboarding document, invoicing instructions, questionnaire, or any other form or document (collectively, "**External Documents**"). No terms or conditions stated in any External Documents will be incorporated into or amend any part of these Terms or result in a new contract between the Parties, even if Armis accepts, clicks through, or completes such External Documents. Armis objects to and rejects all such terms or conditions.

16.11. **Interpretation**. Whenever used in these Terms: (i) the words "include," "includes," and "including" are deemed to be

followed by the words “without limitation”; (ii) the words “hereof,” “hereunder,” “herein,” and similar terms are deemed to mean “under these Terms”; and (iii) the headings in these Terms are for convenience of reference only and will not be used to interpret these Terms.

16.12. **Drafting**. These Terms will be construed without regard to the drafter and will be construed as though each Party to these Terms participated equally in the preparation and drafting of these Terms.

16.13. **Counterparts**. These Terms may be executed in counterparts and may be delivered via electronic transmission, and each counterpart will have the same force and effect as an original and will, together, constitute one and the same agreement. Any electronic signature will have the same effect as a handwritten signature for all purposes, including validity and enforceability.

****

[Signatures on the following page]

If the Parties are executing a signature version of these Terms, the Parties' authorized representatives have agreed to and accepted these Terms as of the last date set forth below.

Customer:	_____	Armis:	_____
Signature:	_____	Signature:	_____
Name (Print):	_____	Name (Print):	_____
Title:	_____	Title:	_____
E-mail:	_____	E-mail:	Legal.notices@Armis.com
Date:	_____	Date:	_____

Armis Platform Support Terms

These Armis Support Terms ("**Support Terms**") detail the customer support services provided by Armis, Inc. ("**Armis**," including any of its affiliates) with respect to the Armis Platform ("**Support Services**" and "**Platform,**" respectively) subscribed to by the Armis customer ("**Customer**") under the Armis Terms and Conditions, including any addendums attached thereto (collectively, "**Terms,**" attached hereto and available at https://www.armis.com/legal-compliance/platform-terms-and-conditions/, or another version of the Terms agreed to in writing among such Customer and Armis). Support Services are expressly conditioned in Customer's ongoing compliance with the Terms, which are attached hereto and incorporated by reference to these Support Terms. Support Services provided to Customer are coterminous with the Subscription Term stated in the Terms or a valid Purchase Order. Armis may non-materially update these Support Terms from time to time as services evolve, in which case provided the updated Support Terms materially similar or improved Support Services, the non-materially updated Support Terms will supersede prior versions. Capitalized terms used but not defined in these Support Terms shall have the meaning ascribed to such terms in the Terms, and in case of any conflict between these Support Terms and the Terms, the terms of the Terms shall control unless otherwise expressly stated in a version of these Support Terms executed by Armis.

In the event Customer has purchased the Platform and Support Services from Armis through an Armis authorized Partner, Customer shall be entitled to all the rights set forth herein and related to the Support Services purchased by Customer (subject to cases where support services are provided by the Partner) if Customer is the original subscriber to the Platform, has provided with its subscription to the Platform accurate, current and complete Customer information to Armis or the Partner, and maintains and updates such information to keep it accurate, current, and complete during Customer's Subscription Term.

1. Definitions

1.1 "**Action Plan**" means a formal verbal or written description of the tasks to be undertaken by Armis and Customer to diagnose, triage, and address a support issue, along with an approximate timeframe for the processing and completion of tasks.

1.2 "**Actual Platform Availability**" will be calculated on a monthly basis using the following formula: [(Total Scheduled Availability *minus* Downtime Incidents) *divided by* Total Scheduled Availability] *multiplied by* 100%.

1.3 "Downtime" means any time in which the Platform is unavailable to the Customer as measured and determined by Armis via its Platform availability monitoring systems.

1.4 "**Downtime Incident"** means any incident in which Downtime occurs, excluding any Scheduled Downtime and any Downtime resulting from SLA Exclusions.

1.5 "Downtime Notice" means at least five (5) days' prior written notice of any scheduled maintenance outside Maintenance Window or sixty (60) minutes' advance written notice for unscheduled, emergency maintenance (including for emergency fixes, patching or cyber-attacks on the Platform).

1.6 "Force Majeure Event(s)" means circumstances beyond Armis' reasonable control, such as, but not limited to, acts of God, acts of government, acts of terror or civil unrest, or technical failures beyond Armis' control.

1.7 "Initial Support Request" means a support request submitted by a Customer's representative contact or their designated Partner to report a suspected Malfunction.

1.8 **"Maintenance"** means downtime during a Maintenance Window

1.9 "**Maintenance Window**" means Sunday between 10AM UTC +3 and 6PM UTC +3.

1.10 "**Malfunction**" means any error or other condition that prevents the Platform from performing substantially in accordance with the operating specifications in the then current Documentation, as measured and determined by Armis via its availability monitoring systems, but excluding a Malfunction Exception.

1.11 "**Malfunction Exception**" means Platform component Malfunction caused by, related to or arising out of (i) any abuse, misuse or unauthorized use of the Platform (including unapproved modifications or adjustments to the Platform) by the Customer other than in accordance with the Documentation or any other agreement among Armis and Customer for the use of the Platform; (ii) an unauthorized combination of the Platform with any software or hardware components or other item not reasonably expected to be combined with and/or interoperate with the Platform, or an interoperability issue beyond Armis' reasonable control, (iii) any technology issues originating from Customer or a third party not under Armis' control; or (iv) any fault or misconfiguration in any equipment or third party software that are not provided by Armis but are used by Customer in conjunction with the Platform.

1.12 "**Resolution**" means a temporary workaround solution or a configuration that renders the Platform reasonably functional for their intended purpose, or a solution that renders the Platform substantially in conformity with the Documentation.

1.13 "**Response**" means Armis' personnel response via outbound e-mail, web or phone consultation (based on the Support Plan subscribed to by Customer) to a designated Customer support contact, acknowledging receipt of an Initial Support request.

1.14 "**Response Time**" means the elapsed time between the Initial Support Request and the target time for a Response during Support Hours.

1.15 **"SLA Exclusions"** means factors outside of Armis' reasonable control, including without limitations: (i) any Force Majeure Event; (ii) any technology issue originating from Customer or a third party not under Armis' control; or (iii) any breach of the Armis Terms & Conditions by Customer.

1.16 **"Scheduled Downtime"** means downtime during a Maintenance Window, or planned or emergency downtime outside a Maintenance Window for which Armis provides Downtime Notice, which together shall not exceed six (6) hours per month.

1.17 **"Support Hours"** means 9 hours (from 5:00am UTC till 24:00am UTC during weekdays for Standard Support and 24X7/365 for Premium and Platinum Support.

1.18 **"Support Plan(s)"** means the different support tiers of Standard, Premium, and Platinum Support, offered by Armis to customers, as further detailed in these Support Terms and related Documentation, and as stated in each case in a relevant Quote or Purchase Order.

1.19 "**Total Scheduled Availability**" means 7 days per week, 24 hours per day during a calendar month, minus Scheduled Downtime and Downtime resulting from SLA Exclusions.

1.20 **"Version"** means generally available (GA) release of Platform software designated by the number which is immediately to the left or right of the left-most decimal point in an Armis version number, as follows: (x).x.x or x.(x).x.

2. Scope of Support Services

2.1 Armis provides Support Services for its most current Version of the Platform, and the

immediately preceding Version of the Armis Platform; provided that Customer is in compliance with all of the terms of these Support Terms and the Terms, and has paid all applicable Fees when due, Armis will provide to Customer the Support Services set forth herein, and upon Customer's request, Armis will report on the status of the Support Services requested by Customer.

2.2 During the Support Hours detailed for the applicable Support Plan, Armis will (i) provide technical support to Customer through Armis' designated support systems, including a support portal and designated telephone number, and (ii) exert all reasonable efforts to provide Resolution, in each of (i) and (ii) as further detailed in the Support Levels and Response Times table below ("**Support Table**") (all Support Services provided in English). Support Services do not include: (x) except for Collectors, support with respect to hardware on which the Platform or any portion thereof may be installed, (y) support with respect to Malfunction Exception, or (z) any monitoring and/or incident response services. Armis has no obligation to develop any particular Resolution, and products/solutions marketed by Armis as separate products for which additional fee is generally charged, are not considered a Resolution.

2.3 Except as otherwise stated in a Purchase Order executed by Armis or otherwise mirroring the support terms detailed in a corresponding Armis Quote, Armis will provide Support Services at no additional charge.

3. Technical Case Workflow.

3.1 Before contacting Armis with an Initial Support Request or with a suspected Malfunction, Customer undertakes to: (i) analyze the Malfunction to determine if it is the result of Customer's misuse, the performance of a third party or some other Malfunction Exception or cause beyond Armis' reasonable control, (ii) ascertain that the Malfunction can be replicated, and (iii) collect and provide to Armis all relevant information relating to the Malfunction.

3.2 Armis support personnel will provide Customer Support Services via remote assistance to identify and determine Malfunctions, produce reports of Malfunctions, and attempt to help the operation of the Armis Platform in light of Malfunctions.

3.3 Upon receiving Customer's Initial Support Request, Armis' qualified personnel will use commercially reasonable efforts to provide a Response within the Response Time and communication channels detailed in the Support Table below. For Severity 1 issues, Response Time will be measured from Customer's phone call. Following the initial Response, Armis support representative will explore the nature of the Malfunction experienced by Customer and its effect on the Platform, and assign a severity level to the Malfunction in accordance with definitions in the Support Table. A Response Time is a guarantee of communication timeframes, and Armis does not guarantee a Resolution within these timeframes. Armis will make commercial reasonable efforts to reach an Action Plan within a reasonable time after the Initial Response.

4. Severity Levels, Response Times, Path to Resolution.

Support Table

Severity	Description	Standard Support Response Time (within 95% of the time during each calendar month)	Premium Support Response Time (within 95% of the time during each calendar month)	Platinum Support Response Time (within 95% of the time during each calendar month)
Severity 1	A malfunction that causes Customer's Platform instance to (a) fail completely, (b) be unoperational or intermittently operational in respect to most functionalities, or (c) materially fail by being inaccessible to a majority of Customer's users.	**Initial Support Request via** Web Submission (support portal or in-product) followed by phone call 4 hours from phone call Work continuously until Resolution is achieved Update every 4 hours until Resolution is achieved	**Initial Support Request via** Web Submission (support portal or in-product) followed by phone call 2 hours from phone call Work continuously until Resolution is achieved Update every 2 hours until Resolution is achieved	**Initial Support Request via** Web Submission (support portal or in-product) followed by phone call 1 hour from phone call Work continuously until Resolution is achieved. If no Resolution within 12 hours of Initial Response Time, Vice President for Support (or similar position) will be paged, and support escalated to Tier 3 Support. If not resolved within 24 hours of Initial Response Time, Chief Customer Officer (or similar position) will be paged Update every 2 hours until Resolution is achieved
Severity 2	Major services/ components are non-functional in Customer's Platform instance, or a subset of users cannot access critical functionality within the Customer's Platform instance, with no reasonable workaround available	**Initial Support Request:** Web Submission 12 hours Work continuously until Resolution is achieved Update every 24 hours until Action Plan is established	**Initial Support Request:** Web Submission 9 hours Work continuously until Resolution is achieved Update every 12 hours until Action Plan is established	**Initial Support Request:** Web Submission 6 hours Work continuously until Resolution is achieved Update every 12 hours until Action Plan is established

Severity	Description	Standard Support Response Time (within 95% of the time during each calendar month)	Premium Support Response Time (within 95% of the time during each calendar month)	Platinum Support Response Time (within 95% of the time during each calendar month)
Severity 3	A malfunction that has a minor impact on a small number of users in Customer's Platform instance, or affects a non production environment or collector, where an acceptable Resolution is available.	**Initial Support Request:** Web Submission 72 hours Work continuously during business hours until Resolution is achieved	**Initial Support Request:** Web Submission 48 hours Work continuously during business hours until Resolution is achieved	**Initial Support Request:** Web Submission 24 hours Work continuously during business hours until Resolution is achieved
Severity 4	All other issues, including minor issues that do not impact Platform functionality, and general how-to questions when a minor issue affects usability or the administration of Customer's production environment.	**Initial Support Request:** Web Submission 6 days	**Initial Support Request:** Web Submission 4 days	**Initial Support Request:** Web Submission 2 days

5. Armis' Technical Support Levels.

5.1 Tier 1 Support:

(i) Initial point of contact for Support Services receives Initial Support Requests.

(ii) Provides basic troubleshooting and attempts to resolve the reported Malfunctions promptly.

(iii) If the reported Malfunctions cannot be resolved within the defined initial response time for the severity level, escalate to Tier 2 Support.

(iv) If the customer experiences a Severity 1 issue, escalate to Tier 2 Support immediately.

5.2 Tier 2 Support:

(i) Handle more complex Malfunctions that Tier 1 Support cannot resolve.

(ii) In-depth troubleshooting and analysis of reported Malfunctions.

(iii) Provide advanced technical support and solutions.

(iv) If Tier 2 cannot resolve the issue within 4 hours for Severity 1 issues, escalate to Tier 3.

(v) If the Malfunction is identified as a critical system outage, escalate to Tier 3 immediately.

5.3 Tier 3 Support:

(i) Handle more complex Malfunctions that Tier 2 Support cannot resolve.

(ii) In-depth troubleshooting and analysis of reported Malfunctions.

(iii) Provide advanced technical support and solutions including direct to R&D interactions.

6. Platform Availability. Armis will provide 99.9% Platform availability over any calendar month as measured by Armis' Platform availability monitoring systems (the "**Platform Availability**"), excluding Scheduled Downtime and Force Majeure Events.

7. Reporting. During the term of the Terms, Armis will, upon Customer's request through Customer's support portal, provide reports to Customer that include Customer's performance with respect to Platform Availability and related metrics as reasonably requested by Customer from time to time.

8. Remedies. If Armis fails to maintain the Support Services Response Time or Platform Availability goals during any three (3) consecutive calendar months during the Subscription Term, then Customer's only remedy is to stop using the Platform, terminate the Terms among Customer and Armis, and receive any prepaid and unused fees for the reminder of the applicable Subscription Term following the effective date of such termination.

9. Cooperation and Governance. In order to achieve the Support Service Response Time goals for Support Services detailed above, the Customer representative must contact Armis Support via the communication methods designated by Armis for submission of Support Services requests. Armis will make available to Customer a single point of contact to cooperate with Customer and respond to any Customer requests with respect to verifying Service Levels and provide such information as may be reasonably requested by Customer to help Customer in resolving issues related to Service Levels. Armis and Customer will hold regular meetings to review and assess Armis' resiliency, recovery and performance targets, address any Customer concerns, and work in good faith to resolve any disputes between the Parties with respect to any Malfunction, Support Services, and related Resolution(s).

ARMIS API & SDK LICENSE AGREEMENT

This Armis API & SDK License Agreement ("**Agreement**") is between Armis, Inc. or one of its affiliates ("**Armis**") and the company or other legal entity ("**Licensee**") whose information is detailed in the signature box below, or who otherwise accepts the terms of this Agreement in one of the ways detailed below. The individual accepting these terms and conditions on behalf of the Licensee represents and warrants that he or she has full authority to bind such company to the Agreement.

This is a legal, enforceable contract between Licensee and Armis, and by executing this Agreement, or by executing this Agreement or order incorporating this Agreement (or a negotiated version thereof, which if co-signed by Armis then such version shall supersede any electronic version of this Agreement), as the case may be (and such time "Effective Date"), Licensee agrees to be bound by the terms of this Agreement. If the individual signing, accepting or clicking through this Agreement (or using the API/SDK) is entering this Agreement on behalf of another entity (or person), such individual represents to Armis that they are an authorized user with authority to bind Licensee to this Agreement. If such individual does not have such authority or if the Licensee does not agree to this Agreement, Licensee may not use or access the API code and/or SDK.

In consideration of the covenants contained in this Agreement, and for other good and valuable consideration, the Parties agree as follows:

1. Definitions.

1.1. "**APIs**" means one or more application programming interfaces and any accompanying routines, protocols, executable applications and other materials made available by Armis, that allows Licensee products to interact with Armis products and services in accordance with the Documentation as well as Armis' guidance as may be provided to Licensee in writing from time to time.

1.2. "**Application(s)**" means any software application, platform, website, or other interface that Licensee owns or licenses and that interacts with the API.

1.3. "**Developer Materials**" means, collectively, SDKs, APIs, Documentation, Non-Production Access and any applications, source code, updates and upgrades, tools, materials and/or content made available to Licensee by Armis from time to time in connection therewith. Armis may update, modify and/or remove Developer Materials at any time, and may impose limits on certain features and materials offered, or restrict Licensee's access to parts or all of Developer Materials without notice or liability.

1.4. "**Documentation**" means Armis' explanatory notes, technical user guides, installation instructions, articles or similar documents or other written guidance from time to time that Armis makes available to Licensee pertaining to and for the use of the API or SDK (as the case may be).

1.5. **"Intellectual Property Rights**" means all patents, copyrights, moral rights, trademarks, trade secrets and any other form of intellectual property rights recognized in any jurisdiction, including applications and registrations for any of the foregoing.

1.6. **"Non-Production Purposes"** means the sole purpose of internal development, testing and support of integration or interoperability between the Applications and the Platform in accordance with the Documentation.

1.7. "**Open Source Code**" means a software program that is licensed under terms that require disclosure to parties (other than the licensor) of the source materials of the software program or modifications thereof, or any source materials of any other software program with which the Open Source Code software program is intended to operate, or that create obligations to distribute any portions of any software program with which the Open Source Code software program is used)

1.8. "**Privacy Policy**" Armis' Privacy Policy attached hereto.

1.9. **"Platform"** means Armis' proprietary cloud-based SaaS platform, and other components associated thereto and offered by Armis over time, together with the software underlying such products and services and any updates, patches, bug fixes and versions.

1.10. "**Armis SDK**" or "**SDK**" means the Armis software development kit which may include object code, libraries, tools, Sample Code, and any upgrades, modifications, updates, additions and copies thereto, and all Documentation included with such items.

1.11. "**Sample Code**" means software code in source code format designated as "Sample Code" or similar that is included as part of the SDK.

1.12. "**SLA/SLO**" means the Armis Service Level Agreement/Service Level Objectives, as non-materially updated from time to time, attached hereto and available via Armis' Trust Portal.

1.13. **"Subscriber(s)"** means customers of Armis with an active subscription with Armis to use the Platform.

1.14. "**User Data**" means all data and information which is uploaded to, processed by, and/or stored within the Platform by a Subscriber.

2. Purpose and License Rights.

2.1. Subject to Licensee's compliance with the terms and conditions of this Agreement, Armis hereby grants to Licensee a limited non-exclusive, non-transferable, non-sublicensable, revocable, fully paid-up, royalty free, world-wide license to: i) access, use and write to the APIs solely to enable the interoperability of the Applications with the Platform; ii) enable and distribute the Application(s) as integrated with the Platform to its end-user customers who are also Subscribers; iii) access and use an instance of the Platform ("**Non-Production Access**"); iv) install and use a limited number of copies of the SDK on computers owned or controlled by Licensee, solely in connection with and as necessary to develop and test the integration of Applications with the Platform, to be used by Licensee's employees or consultants as provided herein, and not for general business purposes, and such employees or consultants shall be subject to the same obligations and restrictions under this Agreement; and v) use, modify or merge all or portions of the Sample Code with Licensee's Applications and distribute it to Subscribers only as part of Licensee's products in object code form, in each case solely a) for Non-Production Purposes, and b) in accordance with the applicable Documentation. Any modified or merged portion of the Sample Code is subject to this Agreement.

2.2. This Agreement does not govern Licensee's use of the Platform. Any use of the Platform is subject to and governed by the Armis Terms & Conditions attached hereto and available at https://www.armis.com/legal-compliance/.

2.3. Licensee acknowledges and agrees that Armis may, in its sole discretion, limit the rate at which Subscribers may access and use the API ("**API Limits**"). Such limitations may be implemented to ensure fair use, optimize performance, or protect the API's infrastructure. Armis may modify these limits at any time, with or without notice, provided that modified limits shall not materially degrade functionality that Licensee has contracted for.

3. License Restrictions and Obligations.

3.1. Except as expressly provided for in this Agreement, Licensee may not conduct, cause or permit the: (i) sale, assignment, distribution, publishing, use, copying, modification, rental, lease, sublease, sublicense, transfer of or otherwise make available the Developer Materials to any third party; (ii) access or use the Developer Materials or Platform in any manner or for any purpose that infringes, misappropriates, or otherwise violates any intellectual property right or other right of any third party, or that violates any applicable law or regulation; (iii) access or use the Developer Materials, or Platform for the development, provision, or use of a software service or product that competes with any of Armis' services or products; (iv) use of the Developer Materials, Armis Confidential Information, the Platform or any components of the Platform subject to Armis Intellectual Property Rights for the purpose of creating any derivative works based on the Platform, or Developer Materials, or otherwise to substantially replicate and/or offer any products, products components or services offered by Armis; (v) reverse engineering, disassembly, or decompiling, deriving source code, extracting underlying design, ideas, operation or structure of the Developer Materials (except that Licensee may decompile the API for the purposes of interoperability with the Applications) or Platform; (vi) use the Developer Materials in any way that would undermine the security of customer data hosted by the Platform on behalf of customers; (vii) defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any protection mechanisms of the Platform or Developer Materials; (viii) input, upload, transmit, or otherwise provide to or through the Developer Materials any information or materials that are unlawful or injurious, or contain, transmit, or activate any malicious or harmful code; (ix) remove, delete, alter, or obscure any copyright, trademark, patent, or other intellectual property or proprietary rights notices in or relating to the Platform, or Developer Materials; (x) modification of the API and/or the SDK in any manner that would cause the API and/or the SDK in whole or in part to become Open Source Code; (xi) access or use of the Developer Materials in order to monitor the availability, performance, or functionality of the Platform or Developer Materials for any benchmarking purposes, (xii) display any form of advertising within or connected to the API as received by any Subscriber of the Platform, (xiii) include any portion of the SDK in Licensee's developer products, or (ix) use the API

in excess of the API Limits. Armis retains all rights that are not expressly licensed to Licensee in this Agreement and Armis does not grant Licensee any implied license in this Agreement under any theory.

3.2. Licensee may not use the Armis Platform and related service names, trademarks, service marks, branding and logos in any way except as agreed by Armis in writing and where such permission is granted such use shall be in accordance with Armis Trademark Guidelines ("**Guidelines**") found at https://www.armis.com/legal (as may be amended by Armis from time to time).

3.3. Except as permitted in section 8.2, Licensee shall not make any modifications to User Data, other than as reasonably necessary to modify the formatting of such User Data in order to display it in a manner appropriate for the pertinent Applications.

3.4. Licensee acknowledges that Armis has no responsibility or liability of any kind, and that Licensee is solely responsible for (i) the content, development, installation, operation, support or maintenance of Applications(ii) creating and displaying information and content on, through or within Application; (iii) ensuring that Licensee's Application does not violate or infringe the Intellectual Property Rights of any third party; (iv) ensuring that Application is not offensive, profane, obscene, libelous or otherwise illegal; (v) ensuring that Licensee's Application does not contain or introduce Malicious Software into the Platform, the Developer Materials, User Data, or other data stored or transmitted using the Platform; (vi) ensuring that Licensee's Application is not designed to or utilized for the purpose other than what is clearly presented and described to Armis customers (v) ensuring that its Application does not violate any applicable law or third party right and (vi) ensuring that Licensee and each Subscriber have a valid agreement among them for the subscription by Subscriber to Licensee's Application which includes clear permission by Subscriber to Licensee to interconnect the Platform to any relevant Application, and extract and use User's Data as necessary for the operation of the Application in accordance with the applicable documentation agreed upon by such Subscriber. "**Malicious Software**" means any software intentionally designed to cause damage to other software, a computer, server, client, or computer network and includes without limitation locks, viruses, trojans, worms, spyware, adware, copy protect mechanisms, back doors, other malware and malicious code designed to permit unauthorized access to the Platform, Developer Materials, User Data or to any Armis networks, systems, programs, or data.

3.5. Licensee will respect and comply with the technical and policy-implemented limitations of the API and SDK, and the restrictions of this Agreement in designing and implementing Applications including, without limitations, any explicit rate limitations on calling or otherwise utilizing the API or SDK.

4. Ownership.

4.1. Subject only to the license rights expressly granted to Licensee under this Agreement, the Platform, Developer Materials, and all data and information contained therein, and any worldwide copyrights, trademarks, trade secrets, patents, patent applications, moral rights, contract rights, and other proprietary rights relating thereto, are the proprietary property of Armis or its licensors and are protected by intellectual property laws, including copyright and patent laws. Armis and its licensors retain any and all rights, title and interest in and to the Platform and Developer Materials, including in all copies, improvements, enhancements, modifications and derivative works of the Platform and Developer Materials. Licensee's rights to use the Developer Materials shall be limited to those expressly granted in this Agreement.

4.2. Any third party components ("**Third Party Components**") that may be included in the Platform or Developer Materials under open source or other software licenses do not alter any rights or obligations Licensee may have under those open source or other software licenses. Notwithstanding anything to the contrary contained in such licenses, the disclaimer of warranties and the limitation of liability provisions in this Agreement shall apply to such Third Party Components.

4.3 Licensee may provide Armis with verbal and/or written Feedback, and hereby assigns all right, title, and interest in the Feedback to Armis, including all Intellectual Property Rights therein. "**Feedback**" means suggestions, comments, reports, or other feedback provided by Licensee or its agents to Armis related to your use of the Platform or Developer Materials. Armis acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

5. Support and Maintenance.

Licensee agrees to report to Armis any bugs or technical issues with the API or SDK and Armis will use commercially reasonable efforts to correct any such issues in accordance with Armis' SLA/SLO. Armis does not otherwise offer support or maintenance for the API or SDK. Licensee is solely responsible for providing all support and technical assistance to users of its Applications. Licensee agrees to use commercially reasonable efforts to provide reasonable support to users of its Applications.

6. Modifications.

Licensee acknowledges and agrees that Armis may from time to time non-materially modify the Developer Materials, this API Agreement and/or the Privacy Policy (each, a "**Modification**"). Licensee acknowledges and agrees that any such Modification may be implemented at any time and without any notice to Licensee. If a Modification is provided to Licensee, then Licensee shall, within thirty (30) days from the date of receipt of such Modification (or such shorter period of time if specified by Armis) (the "**Conformance Period**") comply with such Modification(s) by implementing and using the most current version of the API and the SDK and making any changes to Application that may be required as a result of such Modification(s). While Armis may implement Modifications in an effort to continuously improve the quality and features of the API and/or SDK, Licensee acknowledges that a Modification may have an adverse effect on the Application, including but not limited to, changing the manner in which the Application communicates with the API. Armis shall have no liability of any kind to Licensee or any user of the Application with respect to such Modification or any adverse effects resulting from such Modification. Licensee's continued access to or use of the API and/or SDK following the Conformance Period shall constitute binding acceptance of the Modification(s) at issue.

7. Term and Termination.

Armis maintains the right to terminate this Agreement or access to Developer Materials, and accompanying support at any time by providing Licensee with thirty (30) days' written notice. In the event Licensee breaches this Agreement, it will automatically terminate. Upon termination, Licensee's license to the Developer Materials shall terminate and Licensee must immediately stop using the Developer Materials within Licensee's possession or control. The following provisions will survive termination: Section 3 (License Restrictions and Obligations), Section 4 (Ownership), Section 8 (Representations, Warranties and Covenants), Section 9 (Limitation of Liability), Section 10 (Indemnity), Section 12 (Privacy, Security and Data Collection), Section 13 (Confidentiality), and Section 14 (General).

8. Representations, Warranties and Covenants.

8.1. ARMIS WARRANTS THAT THE DEVELOPER MATERIALS WILL PERFORM SUBSTANTIALLY IN ACCORDANCE WITH DEVELOPER MATERIALS WRITTEN MATERIALS ACCOMPANYING IT. EXCEPT AS EXPRESSLY SET FORTH IN THE FOREGOING, THE DEVELOPER MATERIALS ARE PROVIDED "AS IS" AND ARMIS DISCLAIMS ANY AND ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, TITLE, OR ANY OTHER WARRANTY, WHETHER EXPRESSED OR IMPLIED. THERE IS NO WARRANTY THAT THE DEVELOPER MATERIALS WILL BE ERROR FREE. LICENSEE AGREES THAT LICENSEE'S USE OF THE DEVELOPER MATERIALS IS AT LICENSEE'S OWN DISCRETION AND RISK. LICENSEE IS SOLELY RESPONSIBLE FOR ANY DAMAGE TO LICENSEE'S SYSTEM OR ANY LOSS OF DATA THAT RESULTS FROM SUCH USE.

8.2. To the extent Licensee's Applications transmit User Data outside the Platform, Licensee represents and warrants that Licensee has notified and obtained consent from all Subscribers using such Applications that their User Data will be transmitted outside the Platform and that Armis is not responsible for the privacy, security or integrity of such User Data outside the Platform. Licensee further represents and warrants that to the extent Licensee's Applications store, process or transmit User Data, neither Licensee nor Licensee's Application will, without appropriate prior user consent or except to the extent required by applicable law (a) modify the content of User Data in a manner that adversely affects the integrity of User Data; (b) disclose User Data to any third party except with the prior written consent of the relevant Subscriber; or (c) use User Data for any purpose other than providing the Application functionality to Subscribers using such Application. Licensee shall maintain and handle all User Data in accordance with privacy and security measures reasonably adequate to preserve the confidentiality and security of all User Data and all applicable privacy laws and regulations, and in no event less protective than the measures and policies set forth the Privacy Policy.

8.3. Licensee represents, warrants and covenants that (a) its Applications and Licensee Marks, the use of such Applications by its users, and the activities with respect to such Applications and Licensee Marks undertaken by Armis in accordance with the terms of this Agreement, do not and will not violate, misappropriate or infringe upon the Intellectual Property Rights of any third party; (b) Licensee will comply with all applicable local, state, national and international laws and regulations, including, without limitation, all applicable export control laws, and maintain all licenses, permits and other permissions necessary to develop, implement and Publish its Applications; (c) its Applications do not and will not contain or introduce any Malicious Software into the Platform, the Developer Materials, any of User Data, or other data stored or transmitted using the Platform.

9. Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL ARMIS BE LIABLE

TO LICENSEE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, ENHANCED, PUNITIVE, OR SIMILAR INDIRECT DAMAGES, INCLUDING BUT NOT LIMITED TO ANY: (1) INCREASED COSTS, DIMINUTION IN VALUE, OR LOST BUSINESS, PRODUCTION, REVENUES, OR PROFITS; (2) LOSS OF GOODWILL OR REPUTATION; (3) INTERRUPTION OR DELAY OF THE DEVELOPER MATERIALS; (4) LOSS, DAMAGE, CORRUPTION, OR RECOVERY OF DATA, OR BREACH OF DATA OR SYSTEM SECURITY; OR (5) COST OF REPLACEMENT GOODS OR SERVICES, IN EACH CASE REGARDLESS OF WHETHER EITHER PARTY WAS ADVISED OF THE POSSIBILITY THAT SUCH LOSSES OR DAMAGES WERE OTHERWISE FORESEEABLE. THE FOREGOING LIMITATIONS APPLY EVEN IF ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, ARMIS' AGGREGATE LIABILITY TO LICENSEE OR ANY THIRD PARTY ARISING OUT OF OR RELATING TO THIS AGREEMENT, SHALL IN NO EVENT EXCEED ONE HUNDRED U.S. DOLLARS ($100). ANY CLAIM ARISING OUT OF OR RELATING TO THIS AGREEMENT MUST BE BROUGHT WITHIN SIX (6) YEARS OF THE FIRST EVENT OR OCCURRENCE GIVING RISE TO THE CLAIM.

10. Indemnity.

10.1. Subject to the conditions of Section 10.3, Armis shall have the right to intervene to defend Licensee against any claims, suits, actions, or proceedings brought against Licensee to the extent such claim alleges that Customer's permitted Non-Production Access use of the Armis Platform under this Agreement infringes or misappropriates the intellectual property rights of a third party ("**IP Claim**"). Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. Armis shall indemnify Licensee for all damages, fines, judgments, costs, and expenses, including reasonable attorneys' fees, that are finally awarded by a court of competent jurisdiction or that are agreed to by Armis in a monetary settlement in connection with an IP Claim. If any IP Claim is brought or threatened, Armis may, at its sole option and expense: (i) procure for Licensee the right to continue to use the Armis Platform; (ii) modify or replace the relevant portion(s) of the Armis Platform with a non-infringing alternative having substantially equivalent performance; or (iii) terminate this Agreement as to the infringing portion(s) of the Armis Platform. Notwithstanding the foregoing, Armis is not obligated to indemnify or defend any IP Claim to the extent arising from:
(a) any use of the Armis Platform in combination with software, products, or services not provided by Armis or any modification to the Armis Platform by not authorized by Armis; (b) Licensee's failure to use the Armis Platform in accordance with this Agreement; or (c) Licensee data.

10.2. Reserved.

10.3. The Party seeking indemnification shall provide the indemnifying Party: (i) prompt written notice of the claim (provided that failure to provide prompt written notice will not alleviate a Party's indemnification obligations under this Section 10 to the extent any associated delay does not materially prejudice or impair the defense of the related claims); (ii) sole control of the defense and settlement of the claim (except that indemnifying Party's prior written approval will be required for any settlement that reasonably can be expected to require an affirmative obligation of indemnifying Party); and (iii) reasonable cooperation to indemnifying Party and, at indemnifying's request and expense, assistance in the defense or settlement of the claim.

11. Export Compliance.

Licensee acknowledges that the Developer Materials and related technical data and services (collectively "**Controlled Technology**") are subject to U.S. export control and economic sanctions laws, specifically the U.S. Export Administration Regulations (EAR), and the laws of any country where Controlled Technology is imported or re-exported. Licensee agrees to comply with all relevant laws and will not to export any Controlled Technology in contravention to U.S. law nor to any prohibited country, entity, or person for which an export license or other governmental approval is required.

12. Privacy, Security and Data Collection.

12.1 Armis may collect certain usage statistics from the Developer Materials, including but not limited to, unique identifiers, IP addresses, version number, and information on usage ("**Licensee's Information"**). Licensee's Information will be collected, stored, and used in accordance with this Agreement and the Armis' Privacy Policy. Licensee agrees that Licensee is solely responsible for maintaining the confidentiality of Licensee's login information and that Licensee is solely responsible for any actions taken using Licensee login information. Licensee must notify Armis immediately upon discovery of any unauthorized use of Licensee's login information or account. Licensee acknowledges that Armis

uses login information according to this Agreement and the Privacy Policy.

12.2 Licensee shall maintain and handle all such User Data in accordance with published privacy and security measures reasonably adequate to preserve the confidentiality and security of all User Data and all applicable privacy laws and regulations, and in no event less protective than the measures and policies set forth in the Privacy Policy.

13. Confidentiality.

Licensee may from time to time, gain access to Confidential Information. "**Confidential Information**" means all information disclosed (whether in oral, written, or other tangible or intangible form) by one Party (the "**Disclosing Party**") to the other Party (the "**Receiving Party**") concerning or related to this Agreement, the Developer Materials, or the Disclosing Party that is marked as confidential or proprietary, or that the Receiving Party knows or reasonably should know, given the facts and circumstances surrounding the disclosure of the information by the Disclosing Party, is confidential information of the Disclosing Party. Confidential Information includes, but is not limited to, as well as all proprietary and/or non-public technical, business, commercial, financial and/or legal information, such as, without limitation, any and all Developer Materials information generally shared with Licensee and as specifically related to Licensee, Developer Materials information gained by Licensee through use of the Developer Materials, business plans, product information, pricing, financial plans, know how, Licensee's information, strategies, and other similar information, but excluding User Data. Licensee may use Confidential Information only to the extent necessary to exercise its rights under this Agreement. Subject to the express permissions set forth herein, Licensee may not disclose Confidential Information to a third party without the prior express consent of Armis, provided in writing or by email. Without limiting any other obligation of Licensee under this Agreement, Licensee agrees that Licensee will protect Confidential Information from unauthorized use, access, or disclosure in the same manner that Licensee would use to protect Licensee's own confidential and proprietary information of a similar nature and in any event with no less than a reasonable degree of care. Armis recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

14. General.

14.1. **Assignment.** Licensee may not assign the rights granted hereunder or this Agreement, in whole or in part and whether by operation of contract, law or otherwise, without Armis' prior express written consent. Armis may audit Licensee's use of the Developer Materials subject to Government security requirements.

14.2. **Governing Law and Venue.** This Agreement will be governed by and construed in accordance with the Federal laws of theUnited States.

14.3. **Severability.** If any provision of this Agreement is found illegal or unenforceable, such provision shall be enforced to the maximum extent permissible, and remaining provisions of this Agreement shall remain in full force and effect. A waiver of any breach or default under this Agreement shall not constitute a waiver of any other subsequent breach or default.

14.4. **Entire Agreement.** This Agreement is the complete and exclusive agreement between Licensee and Armis relating to the Developer Materials and supersedes any previous or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter.

****

[Signatures on the following page]

ARMIS DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms a part of the Terms (as defined below) between Armis, Inc. (or the Armis Affiliate with whom Customer is entering into the Terms) ("**Armis**") and the Customer whose legal name is indicated in the Terms ("**Customer**"). This DPA details the manner in which Armis will process Personal Data on behalf of Customer in connection with providing the Platform and/or Services.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

1. Definitions

1.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Terms.

Affiliate	means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with a party herein, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
Armis Group	means Armis, Inc. and its Affiliates engaged in the Processing of Personal Data.
CCPA	means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act, and its implementing regulations.
Personal Data	means personal data (as such term or substantially equivalent term is defined in the Data Protection Laws) that is Processed by Armis on behalf of Customer in connection with providing the Platform and Services.
Contracted Processor	means Armis Group member or a Subprocessor.
Data Protection Laws	means all laws and regulations that apply to the Processing of Personal Data under the Terms, including European Data Protection Laws and the laws and regulations of the United States and its states, as amended from time to time, to the extent such laws and regulations apply to the relevant party.
European Data Protection Laws	means (i) the GDPR, (ii) the United Kingdom General Data Protection Regulation (the "UK GDPR"), and (iii) the Swiss Federal Act on Data Protection, each as amended, replaced or superseded from time to time.
GDPR	means EU General Data Protection Regulation 2016/679.
Individual	means an identifiable natural person about whom Personal Data relates.
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
Processing	(including its cognate "Process") means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Restricted Transfer	means a transfer of Personal Data to Armis that would be restricted by European Data Protection Laws in the absence of the Standard Contractual Clauses.
Standard Contractual Clauses (or SCCs)	means (i) the contractual clauses set out in Annex III, and (ii) where the UK GDPR applies, the contractual clauses set out in Annex IV as supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018.
Subprocessor	means any person (including any third party, but excluding an employee of Armis or any of its sub-contractors) appointed by or on behalf of Armis to Process Personal Data on behalf of Customer in

	connection with Customer's subscription to the Platform and/or Customer's receipt of Services under the Terms.
Terms	means the Armis terms and conditions applicable to all use of the Platform and Services available here: **https://www.armis.com/legal-compliance/armis-platform-terms-and-conditions/** or such version of the Terms (or other agreement governing Customer's use of Armis Platform and/or Services) as is separately executed between Armis and a Customer (as the case may be).

1.2 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Processing of Personal Data

2.1 Armis shall:

2.1.1 comply with the Data Protection Laws to which Armis is subject in its provision of the Platform and/or Services to the Customer. Armis is not responsible for complying with Data Protection Laws to the extent that such Data Protection Laws apply to Customer, its Affiliates, and/or its or their users in the access and use of the Platform or receipt of Services.

2.1.2 not Process Personal Data other than in accordance with the Terms and this DPA (the "**Permitted Purpose**"), unless Processing is required by applicable law to which the relevant Contracted Processor is subject, in which case Armis shall to the extent permitted by applicable law inform the Customer of that legal requirement before the relevant Processing of that Personal Data.

2.1.3 not retain, use, disclose or otherwise Process the Personal Data for any purpose other than the Permitted Purpose, or "sell" the Personal Data within the meaning of Data Protection Laws.

2.2 Customer hereby:

2.2.1 instructs Armis (and authorizes Armis to instruct each Subprocessor) to:

2.2.1.1 Process Personal Data; and

2.2.1.2 in particular, transfer Personal Data to any country or territory, as reasonably necessary for the provision of the Platform and the Services and consistent with the Terms; and

2.2.2 warrants and represents (i) that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in Section 2.2.1 on behalf of each relevant Customer Affiliate, and (ii) that it has obtained all necessary consents required under Data Protection Law for Armis to Process Personal Data.

2.3 Annex II to this DPA explains the nature of the Personal Data Processed pursuant to this DPA as well as the subject-matter, purposes and duration of the Processing.

3. Armis Personnel

Armis shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Personal Data, ensuring in each case (i) that access is strictly limited to those individuals who need to know/access the relevant Personal Data, as strictly necessary for the purposes of the Terms, and to comply with applicable laws in the context of that individual's duties to the Contracted Processor, and (ii) that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

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, Armis has implemented and shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including as described in Annex I to this DPA. In the event that Customer intends to upload or access any sensitive Personal Data or other information requiring additional protections under applicable laws ("**Special Information**"), Customer shall evaluate whether the technical and organizational measures described in Annex I are sufficient to protect Special Information. Customer shall not upload any Special Information to the Platform if Customer determines that the technical and organizational measures described at Annex I are insufficient to protect such Special Information in accordance with applicable laws.

5. Subprocessing

5.1 Customer authorizes Armis to appoint (and permit each Subprocessor appointed in accordance with this Section 5 to appoint) Subprocessors. Armis' website (currently posted at: https://www.armis.com/legal-compliance/subprocessors-list/) lists the Subprocessors that are engaged by Armis. Armis will give notice of new Subprocessors by providing an updated copy of the Subprocessors list on its website ("**Notice**"). If, within fourteen (14) days of the Notice, Customer notifies Armis in writing of any objections to the proposed appointment, and further provides commercially reasonable justifications to such objections based on valid concerns regarding such proposed Subprocessor's business practices relating to data protection, then (i) Armis shall work with Customer in good faith to address Customer's objections regarding the new Subprocessor; and (ii) where Customer's concerns cannot be resolved within thirty (30) days from Armis' receipt of Customer's notice, Customer may, within five (5) days following the end of such thirty (30) day period, terminate the Terms with immediate effect by providing Armis with a written notice delivered in accordance with the Terms.

5.2 With respect to each Subprocessor, Armis shall:

5.2.1 before the Subprocessor first Processes Personal Data, carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Personal Data required by the Terms;

5.2.2 ensure that the Processing of Personal Data by the Subprocessor is governed by a written contract imposing data protection terms that require the Subprocessor to protect Personal Data to the standard required by applicable Data Protection Laws (and in substance, to the same standard provided by this DPA);

5.2.3 if that arrangement involves a Restricted Transfer, ensure that an appropriate data transfer mechanism, including the SCCs, is in place at all relevant times to safeguard the Restricted Transfer in accordance with Data Protection Laws; and

5.3 Armis shall ensure that each Subprocessor performs its obligations under Sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Personal Data carried out by that Subprocessor, as if it were party to this DPA in place of Armis.

6. Individual Rights

6.1 Taking into account the nature of the Processing, Armis shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customers' obligations, as reasonably understood by Customer, to respond to requests to exercise Individual rights under the Data Protection Laws.

6.2 Armis shall:

6.2.1 promptly notify Customer if any Contracted Processor receives a request from an Individual under any Data Protection Law with respect to Customer Personal Data to the extent that Armis recognizes the request as relating to Customer; and

6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Customer or the relevant Customer Affiliate or as required by applicable laws to which the Contracted Processor is subject, in which case Armis shall to the extent permitted by applicable laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Armis shall notify Customer without undue delay upon Armis or any Subprocessor becoming aware of a Personal Data Breach affecting Personal Data, providing Customer with sufficient information, to the extent such information is reasonably available, to allow Customer to meet any obligations to report or inform Individuals of the Personal Data Breach under the Data Protection Laws. Such notification shall include at a minimum the following information to the extent such information is reasonably available: (i) the nature of the Personal Data Breach, the categories and numbers of Individuals concerned, and the categories and numbers of Personal Data records concerned; (ii) the name and contact details of Armis' Data Protection Officer or other relevant contact from whom more information may be obtained; (iii) the likely consequences of the Personal Data Breach; and (iv) the measures taken or proposed to be taken to address the Personal Data Breach.

7.2 Armis shall cooperate with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

To the extent required by Data Protection Laws, Armis shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with data protection regulators, which Customer reasonably considers to be required under Data Protection Laws, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Personal Data

9.1 Subject to Sections 9.2 and 9.3 Armis shall promptly and in any event within sixty (60) days of the date of cessation of providing the Platform or any Services involving the Processing of Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of such Personal Data.

9.2 Each Contracted Processor may retain Personal Data to the extent required by applicable laws and only for such period as required by applicable laws, provided that such Personal Data shall remain subject to the terms of this DPA and may only be Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

9.3 Armis shall provide written certification to Customer that it has fully complied with this Section 9 within ten (10) days of receiving Customer's written request to receive such certification.

10. Audit and Records

10.1 Armis shall, in accordance with Data Protection Laws, make available to Customer such information in Armis' possession or control as Customer may reasonably request with a view to demonstrating Armis' compliance with the obligations of data processors under applicable Data Protection Laws in relation to its Processing of Personal Data.

10.2 Customer may exercise its right of audit under applicable Data Protection Laws in relation to Personal Data, through Armis providing:

10.2.1 a SOC 2 Type II report not older than eighteen (18) months, prepared by an independent external auditor demonstrating that Armis' technical and organizational measures are sufficient and in accordance with an accepted industry audit standard; and

10.2.2 additional information in Armis' possession or control to a data protection regulator when it requests or requires additional information in relation to the Processing of Personal Data carried out by Armis under this DPA.

11. Restricted Transfers

11.1 The parties agree that when the transfer of Personal Data from Customer to Armis is a Restricted Transfer, the SCCs shall be deemed incorporated into and form a part of this DPA as follows:

11.1.1 Customer and Armis shall comply with the obligations of a "data exporter" and "data importer," respectively;

11.1.2 Module 2 of the SCCs shall apply to the extent that Customer is a controller of the Personal Data under European Data Protection Laws.

11.1.3 Module 3 of the SCCs shall apply to the extent that Customer is a processor (and Armis is its subprocessor) of Personal Data under European Data Protection Laws.

12. General Terms

12.1 Without prejudice to clause 18 of the SCCs; (i) the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Terms with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity, or termination, or the consequences of its nullity; and (ii) this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Terms.

12.2 Nothing in this DPA reduces Armis' obligations under the Terms in relation to the protection of Personal Data or permits Armis to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Terms. In the event of any conflict or inconsistency between this DPA and the SCCs, the SCCs shall prevail to the extent

of the conflict and relevance of the SCCs to the Processing of the applicable Personal Data.

12.3 Subject to Section 12.2, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Terms and including (except where explicitly agreed otherwise in writing, signed by the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail to the extent of the conflict and relevance of this DPA to the Processing of the applicable Personal Data.

12.4 Any liability associated with failure to comply with this DPA will be subject to the limitations of liability provisions stated in the Terms.

12.5 Customer may, by at least 30 (thirty) calendar days written notice to Armis, from time to time make any variations to the SCCs entered into under Section 11.1, as such variations apply to Restricted Transfers which are subject to a particular Data Protection Law, but only where such variations are required as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law.

12.6 If Customer gives notice under Section 12.5, then (i) Armis shall promptly cooperate (and direct any affected Subprocessors to promptly cooperate) to ensure that equivalent variations are made to any agreement put in place under Section 5.2.3; and (ii) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Armis to protect the Contracted Processors against additional risks associated with the variations made under Section 12.5.

12.7 If Customer gives notice under Section 12.5, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

12.8 Customer shall not require the consent or approval of Customer Affiliate to amend this DPA pursuant to this Section 12.5 or otherwise.

12.9 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

13. United States

13.1 Where (i) Customer is a "business" as defined in applicable U.S. Data Protection Laws (including but not limited to the CCPA) and (ii) Personal Data processed by Armis under the Terms and this DPA is subject to such U.S. Data Protection Laws ("**Relevant Personal Data**"), the Parties agree that Armis is Customer's "service provider" (as defined therein).

13.2 Armis agrees that, except for usage of Relevant Personal Data as necessary to bring and defend claims, to comply with requirements of legal process, to cooperate with regulatory authorities, and to exercise other similar permissible uses to the extent and as expressly provided under applicable Data Protection Laws:

13.2.1 It will Process Relevant Personal Data in accordance with the Terms and this DPA and will not retain, use, share, or disclose Relevant Personal Data for any purpose other than for providing the Platform and Services or in connection with its rights and obligations under the Terms, this DPA, or applicable Data Protection Laws.

13.2.2 It will not "sell" (as such term is defined by U.S. Data Protection Laws) Relevant Personal Data.

13.2.3 If Armis receives a request from an Individual to exercise a right such Individual has under Data Protection Laws in relation to the information relating to such Individual that is contained in, and identified as, Relevant Personal Data, Armis will provide a copy of the request to Customer. For the avoidance of doubt, Customer will be responsible for handling and communicating with Individuals in relation to such requests.

ANNEX I: TECHNICAL AND ORGANIZATIONAL MEASURES

Introduction

Armis' Platform enables customers to discover, assess, and manage all IT, OT and IoT devices on their network, including those that are managed, unmanaged or unknown. It encompasses the following key functions and services:

- Discover all assets.
- Identify risks and gaps.
- Automate enforcement.

The Platform components are built from the ground-up with robust security controls designed to protect collected Customer Data (as defined in the Armis Platform Terms and Conditions ("Terms"). All Customer Data is processed and stored on Armis' or Armis' third party provider's servers located within supported Cloud Services Providers' ("CSP"). Each CSP data center utilizes state-of-the-art information security measures that are SOC2 Type II audited and/or certified under the ISO27001 standards. Customer Data is kept strictly confidential regardless of location including limited information contained within support tickets. Customer Data is never shared with any third-party organization except Armis' appointed third party subprocessors. Our application, databases, networks, and corporate infrastructures are supported by extensive industry security standards and measures, including a range of technical, physical, and administrative measures, to provide quality data security alongside quality product and user experience.

Overview

Armis implements and maintains a multi-layer Information Security Management System (ISMS), in accordance with ISO 27001 guidance. To test the implementation of the controls, Armis has retained the auditing services of a top-tier, independent 3rd party auditor and has undergone a SOC2 Type 2 and ISO 27001 audit. The ISMS provides for controls at multiple levels of data storage, processing, export and/or deletion, access, and transfer. The strategy includes the following key components:

- Armis corporate security policies
- Organizational security
- Security Risk Management Program
- Asset classification and control
- Personnel/Human Resources secure management
- Information Security Awareness
- Cryptography
- Communications Security
- Vendor Security Risk Management
- Change management
- Physical and environmental security
- Operational security
- Security Vulnerability Management
- Access controls
- Secure systems development and maintenance
- Disaster recovery and business continuity
- Corrective action program
- Regulatory compliance

Organizational Security

Armis employs an internal Information Security Team ("Infosec Team"). The Infosec Team is responsible for building, improving, supervising and maintaining customized security infrastructure, the company's perimeter defense systems, security policies, processes and standards, and implementing Armis' overall information security program. Specifically, the Infosec Team performs the following activities:

- Develop, ensure approval, train on, implement, review and continuously improve security policies, processes, standards and measures for Armis' networks, applications, systems, services and practices, by conducting regular security design and implementation-level reviews;
- Provide ongoing assessment and consultation on security risks associated with all systems and activities involving Customer Data, in relation to known and newly found security concerns, as well as any number of projects and possible solutions to security concerns;
- Implement and continuously improve an information security program comprising of a range of data security administrative, technical and physical measures;
- Oversee the implementation of a range of information security technical measures aimed at logging relevant information security signals, scanning relevant systems, controlling access to relevant systems, implementing data encryption and similar technologies, ensuring data availability and backup, controlling and maintaining personal computers used by Company personnel, and operating a Security Operations Center (SOC) to ensure proper analysis and attention to any and all information security alerts;
- Ensure physical security in all Armis offices and other relevant facilities;
- Oversee all information security aspects of a comprehensive vendor management program where proprietary,

confidential and/or Customer Data is involved;

- Adhere to a formal incident response process to quickly recognize, analyze, and remediate information security threats;
- Develop and deliver training for employees on the information security program, information security awareness, and compliance with security policies and process;
- Engage outside security experts to conduct regular security assessments of Armis' infrastructure and applications.

Administrative Security Measures

Policies and Processes:

Armis has developed and implemented a range of documented policies, standards, programs and processes in support of its overall data security program. These include, but not limited to, employee security training process; employee background checks; incoming and departing employees access and related data protection process; access control policy and processes; product vulnerability management and penetration testing, reporting and remediation process; business continuity and disaster recovery process; security incident management standard; confidentiality documentation policy; vulnerability and patch management standards; mobile devices policy; removable media policy; acceptable encryption standard; vendor risk management standard; configuration management standard; data handling policy; media destruction policy, data classification and handling standard, etc.

Security Risk Management: Armis has implemented a security risk management program which is based on the requirements of NIST Risk Management Framework (RMF). The Program defines a systematic and consistent process to ensure that security risks to Armis' Information Assets are identified, analyzed, evaluated and treated. Risk treatment and the risk remaining after treatment (i.e., residual risk) is communicated to risk owners, who decide on acceptable levels of risk, authorize exceptions to this threshold, and drive corrective action when unacceptable risks are discovered.

Acceptable Use Policy: This policy defines the proper configuration, use and maintenance of Company equipment at Armis (including computing devices, software, storage media, networks and other devices).

Asset Management Policy: This policy covers the following aspects:

- Assets associated with information and information processing facilities are identified and an inventory of these assets is listed and maintained;
- Assets maintained in the inventory are assigned an owner;
- Company provided assets are governed by the Acceptable Use Policy;
- All employees and external party users return all the organizational assets in their possession upon termination of their employment, contract or agreement.

Access Control Policy: This policy is based on an employee's job function and role, using Least-Privilege and Need-to-Know concepts to match access privileges to defined responsibilities. By default, Armis employees are granted only limited permission to access company resources, such as email, internal portals, and HR information. Access to Armis' data systems is controlled by authentication and authorization mechanisms. In addition, employees must be in a Armis office, or connected via VPN or Zero trust network (authenticated with user ID + password + pin/token), then login to an internal portal via SSO, before they can connect with a customer management console and/or server. The policy includes the following rules: (i) system owners are responsible for users with access to their systems; (ii) Armis' Information Technology Group acts as a technical admin to all data systems and supervises grant and removal of access rights; and (iii) upon employees change of duties, access rights are changed accordingly.

Data Classification & Handling: all Data (which includes all proprietary, confidential, sensitive and/or customer data) is classified as such and is assigned corresponding processes and policies with respect to access rights, labeling, encryption requirements, maintenance and destruction, transfer methodologies, sharing, logging and monitoring of such Data.

Security Vulnerability Management Policy & Patch management standard: detailed process for testing Armis products and corporate systems for security vulnerabilities, reporting of identified vulnerabilities and a corresponding elimination procedure. The vulnerability management program also includes:

- The Infosec Team constantly monitors vulnerabilities flagged by customers, employees, hired 3rd party assessors and other users of the Platform. The Team undertakes external testing and audits. The Team is responsible for tracking and following on identified vulnerabilities;
- Quarterly network vulnerability scans and annual penetration testing process implemented, which includes testing of the Armis SaaS Platform, corporate environment and all other systems which host and process proprietary information and customer data;
- Application of security patches to production systems on a regular basis;
- Updating all software components and operating systems as part of every application/management console major release;
- Performing Static, Dynamic code analysis & 3rd party library vulnerability scanning before every major release.

Business Continuity & Disaster Recovery Processes: includes the following components:

- Daily backup of all Customer Data: all Customer Data is backed-up daily in our CSP data center, and where available or provided by the CSP, physically located in a different location (availability zone) from where the same Customer Data is originally stored;
- Monitoring process in place to ensure successful ongoing backup;
- Systems capable of restoring customers servers in under 4 hours (RTO) and RPO of 24 hours;
- For Armis' corporate environment: daily backups of all critical servers, a retention policy of backup data for 1 year, performance of periodic restore and backups monitoring, means and processes to enable employees maintain business continuity during a recovery event;
- Annual Disaster recovery plan testing.

Data Backup and Retention/Deletion Policy: All Customer Data and critical business data is backed-up as follows:

- Daily backup of Customer Data: all Customer Data is backed-up daily in our CSP data center different than the primary location where such Customer Data was originally stored, utilizing online snapshot technology;
- All Customer Data (including backups) is deleted or irretrievably destroyed within 60 days of subscription termination to the Platform.

Security Incident Response Process: Armis has put in place a security incident management process for managing security incidents that may affect the confidentiality, integrity, or availability of its systems or data, including Customer Data. The process specifies courses of action, procedures for notification, escalation, mitigation, *post-mortem* investigations after each incident, response process, periodic testing, and documentation. Armis has a dedicated SOC function, which manages & monitors a Security Information & Event Management (SIEM) solution deployed across the organization.

Security and Data Privacy Awareness Training Process: New employee onboarding security training session conducted with each new employee. Employees are provided with security awareness and data privacy training within a month of joining and yearly thereafter. The process also includes ongoing assessment by the Infosec Team of the security training program, including creation of new content, role specific trainings and other updates.

Personal Machines Security Setup: Documented process for setting up personal computers issued to new employees with focus on security updates, applications and settings.

Employee Hiring & Termination Policy: Detailed process for ensuring appropriate access controls to newly hired employees, proper documentation completion by newly hired employees, tailored infosec employee training, return of all data and relevant Company equipment held by departing employees to Armis, and eliminating employees' access to all Armis systems.

Confidentiality Arrangement Policy: Every new employee, or vendor or agent with access to Armis systems, proprietary information or customer data, is required to execute a comprehensive confidential information agreement in which such employee or agent commits to maintain all Armis and Armis customers information in strict confidence and only use such information in providing services to Armis or a Armis Customer.

Vendor Risk Management: All vendor engagements must be approved by Armis, Infosec, Legal, Finance and Procurement Teams, who review each vendor with respect to risk associated with Armis data and risk associated with vendor relations. Vendors are otherwise required to enter comprehensive confidentiality and quality controls commitments, commit to comprehensive information security standards, agree to reasonable vendor audits & respond to annual security vendor risk assessment questionnaire.

Systems Development and Maintenance: Armis' policy continuously considers the security properties and implications of applications, systems, and services used or provided by Armis throughout a given project lifecycle. The policy requires individuals to implement appropriate security measures in applications, systems, and services being developed, commensurate with identified security and concerns. The Company's Infosec Team is responsible for providing security-related guidance and risk assessment. A comprehensive procedure is also in place for code development, code review, Q&A cycle, change request process, code freezing and rollout.

Other Administrative Security Measures

Designated Heads of Information Security Program: The Infosec Team is headed by a designated implementation lead, working closely with a compliance lead to define and execute information security program goals.

Geography-based Customer Data Processing/Storage: Armis has implemented an infrastructure configuration whereby customers may select to store all management console data in certain data centers located in geographies selected by customers.

Internal Audit Program: Armis has implemented an internal audit program, to ensure an organized audit process for the Company's information security policies, processes, technical measures and practices.

Personnel Security: Armis utilizes a 3rd party service to perform comprehensive background checks of all new hires and contractors with access to customer data, subject to local law limitations. Such background checks, as allowed by local laws, include criminal history, prior employment, educational background and reference checks.

Technical Security Measures

Encryption Practices: All communications with Armis servers, and among Armis servers in different locations, is encrypted in transmission. 256 bit TLS 1.2 is supported. All password information is encrypted at rest. In addition, all customers data is encrypted at rest using AES 256.

Network Security: Customers management consoles servers are isolated such that no access is possible among servers of different customers. The Armis network is protected by redundant firewalls, commercial-class router technology, regular audits, and a host intrusion detection system on the firewall that monitors malicious traffic and network attacks.

Vulnerability Assessment and Pen-Testing: Armis conducts annual, comprehensive penetration testing by a top-tier third party service, including penetration testing our SAAS and agents (black and grey box), corporate infrastructure penetration testing and social targeted attack, and public website automatic testing for open vulnerabilities. A licensed tool is used to perform quarterly network vulnerability assessment on all servers in corporate networks as well as CSP cloud.

MFA: Multi-factor authentication is enabled for access to all critical systems, as well as all admin-level accounts.

Multi-factor authentication and Single-Sign-On (SAML2) systems are implemented with respect to all in-product accesses, as well as Company security devices.

Physical Security Measures

Data Center Perimeter Security: Armis utilizes fully managed data centers from Amazon Web Services (AWS). These data centers are geographically distributed and employ a variety of best-in-class physical security measures. The standard physical security controls at each Data Center consist of reliable, well-tested technologies that follow generally accepted industry best practices: custom-designed electronic card access control systems, alarm systems, biometric identification systems, interior and exterior cameras, and a 24X7X365 presence of security guards. Access to areas where systems or system components are installed or stored is restricted to personnel whose identities are verified through biometric security measures and who have gone through background checks. Such areas are segregated from general office and public areas.

Access to Armis offices is protected via custom-designed electronic card access control systems including individually-assigned cards and access logging, round-the-clock interior and exterior surveillance, close circuit cameras and alarm systems. We also maintain important contact information with local emergency agencies.

Data Privacy

Because Armis' collection of assets data and activity is focused on system-level analysis, the majority of the data Armis collects does not include any personally identifiable information, or information which may lead to the identification of a unique individual (PII). The Customer Data collected by the Platform that may constitute PII including: assets ID and User Names (as assigned by Customers' IT function); limited number of customers employees' names, emails (for admin login purposes as well as communication and alerts to customers' admins); IP addresses.

As part of its data privacy compliance plan, Armis has implemented a system configuration which allows customers to choose specific geographic data centers where they can store all management console data. For example, European customers can choose to store all their management console data in Armis' CSP data centers in Frankfurt, Germany.

Armis continuously updates its Privacy Policy and privacy practices, achieving timely compliance with the European General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) and implementing a host of data privacy compliance steps to ensure continued compliance with prevalent data privacy legislation. Such practices include, among other things, accountable management of all PII processed by Armis on behalf of its customers and employees, mapping and documentation of all PII processing, privacy-specific training, breach notification/remediation process, PII access/review/export requests policy and process, appointment of a data privacy officer, permanent deletion of PII once no longer needed to provide the Armis Solutions, and continuous monitoring of emerging data privacy legislation in geographies where Armis does business.

ANNEX II: DETAILS OF PROCESSING OF PERSONAL DATA

Subject Matter	Armis will Process Personal Data as necessary to provide the Platform and Services pursuant to the Terms.
Duration	For the duration of the provision of the Platform and Services, in accordance with the Terms.
Nature and Purpose	Armis will store, process and access Personal Data to the extent reasonably necessary to provide Customer the Platform (and/or Services) and to create System Data to improve the Platform.
Categories of Data Subjects	1. Customer's and/or its Affiliates' employees, contractors and points of contact. 2. Customer's and/or its Affiliates' personnel, staff and contractors (and other individuals) connecting devices to Customer and/or its Affiliates' (or their customers') networks monitored by Armis.
Categories of Personal Data	1. Names 2. Usernames 3. Email addresses 4. Device Identifiers (host names, IP address, Mac address, geolocation data).
Sensitive / Special Data	N/A. The Platform is not intended to Process special / sensitive categories of data.

ANNEX III

STANDARD CONTRACTUAL CLAUSES

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) for the transfer of personal 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 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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.

MODULE ONE: Transfer controller to controller

8.1 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;
(ii) where necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
  (i) of its identity and contact details;
  (ii) of the categories of personal data processed;
  (iii) of the right to obtain a copy of these Clauses;
  (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. I t shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they 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 subject. 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.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefiting 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 of Regulation (EU) 2016/679 with respect to the processing in question;
(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

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 (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 benefiting 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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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 benefiting 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 of Regulation (EU) 2016/679;
(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of

implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION 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 fourteen (14) 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. The Parties agree that, by complying with this Clause, the data importer fulfills 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 fulfill 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.

MODULE THREE: Transfer processor to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that li st through the addition or replacement of sub-processors at least fourteen (14) days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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. The Parties agree that, by complying with this Clause, the data importer fulfill s 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;
(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(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.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has receiv ed from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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 it s 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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-*

controller with personal data collected by the processor in the EU)

(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;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;

(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;

(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). [For Module Three: The data exporter shall forward the notification to the controller.]

(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 [for Module Three:, if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

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.

[For Module Three: The data exporter shall forward the notification to the controller.]

(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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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 [for Module Three: and the controller] 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) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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 Ireland.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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 Ireland.

(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.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of Ireland.

ANNEX I to SCC

A. LIST OF PARTIES

Data importer:

- Name: Armis Inc. or the Armis Affiliate with whom Customer is entering into the Terms
- Address: 548 Market Street, Suite 97439, San Francisco, CA 94104-5401 (or as set out in the Terms).
- Contact person's name, position and contact details: Legal Department, privacy@Armis.com
- Activities relevant to the data transferred under these Clauses: Armis' Platform enables customers to discover, assess, and manage all IT, OT and IoT devices on the Customer network, including those that are managed, unmanaged or unknown.
- Signature and date: Please see the signature and date of the DPA
- Role (controller/processor): Processor

Data exporter:

- Name: Customer
- Address: As identified in the Purchase Order
- Contact person's name, position and contact details: As identified in the Purchase Order
- Activities relevant to the data transferred under these Clauses: Transfer of Customer's users' credentials of Armis' cybersecurity platform and Customer information system data as required to utilize the Armis Platform to discover, assess, and manage all IT, OT and IoT devices on the Customer network, including those that are managed, unmanaged, and unknown.
- Signature and date: Please see the signature and date of the DPA
- Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: See Annex II.

Categories of personal data transferrer: See Annex II.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved: See Annex II.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Transfer of data is continuous as per the term of the Terms.

Nature and purpose of the processing: See Annex II.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Personal Data will be retained for as long as necessary taking into account the purpose of the Processing, and in compliance with applicable laws, including laws on the statute of limitations and Data Protection Laws.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: For the subject matter and nature of the Processing, reference is made to the Terms and this DPA. The Processing will take place for the duration of the Terms.

C. COMPETENT SUPERVISORY AUTHORITY

*Identify the competent supervisory authority/ies in accordance with Clause 13: Where the Customer is based in an EU Member State, t*he supervisory authority of the country where the Customer is based shall act as competent supervisory authority.

ANNEX II to SCC

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons: See Annex I.

and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Armis requires its subprocessors to comply with materially equivalent technical and organizational measures as those adopted by Armis.

ANNEX IV

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables
Table 1: Parties

Start date	**As above.**	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	**See all details above.** **Full legal name:** **Trading name (if different):** **Main address (if a company registered address):** **Official registration number (if any) (company number or similar identifier):**	**See all details above.** **Full legal name:** **Trading name (if different):** **Main address (if a company registered address):** **Official registration number (if any) (company number or similar identifier):**
Key Contact	**See all details above.** **Full Name (optional):** **Title:** **Contact details including email:**	**See all details above.** **Full Name (optional):** **Job Title:** **Contact details including email:**
Signature (if required for the purposes of Section 2)	**See above.**	**See above.**
Addendum EU SCCs	**The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:** **Date: See all details above.** **Reference (if any):** **Other identifier (if any):**	

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See above.
Annex 1B: Description of Transfer: See above.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See above.

Annex III: List of Sub processors (Modules 2 and 3 only): See above.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	**Which Parties may end this Addendum as set out in Section 19:** **Importer - YES** **Exporter - YES**

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	**This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.**
Addendum EU SCCs	**The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.**
Appendix Information	**As set out in Table 3.**
Appropriate Safeguards	**The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.**
Approved Addendum	**The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.**
Approved EU SCCs	**The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.**
ICO	**The Information Commissioner.**
Restricted Transfer	**A transfer which is covered by Chapter V of the UK GDPR.**
UK	**The United Kingdom of Great Britain and Northern Ireland.**
UK Data Protection Laws	**All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.**

UK GDPR	**As defined in section 3 of the Data Protection Act 2018.**

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re- enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:
"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";

c. Clause 6 (Description of the transfer(s)) is replaced with:
"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:
"it is to a country benefiting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:
"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:
"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:
"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:
"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:
    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

When executed via physical signatures:

IN WITNESS WHEREOF, the Parties' authorized representatives have executed this Armis API and SDK License Agreement).

LICENSEE: _____	**ARMIS INC.**
Signature: _____	Signature: _____
Name (Print): _____	Name (Print): _____
Title: _____	Title: _____
Address: _____	Address: 548 Market Street, Suite 97439San Francisco, CA 94104-5401
E-mail: _____	E-mail: Legal.notices@armis.com
Date Signed: _____	Date Signed: _____

INTELLIGENCE CENTER AND EARLY WARNING

ADDENDUM TO ARMIS PLATFORM TERMS AND CONDITIONS

This Intelligence Center and Early Warning Addendum ("**Addendum**") to the Armis Platform Terms and Conditions ("**Terms**," hereto attached), unless another version of the Terms is entered into in writing among Armis and Customer (each, as defined below)) forms a part of the Terms between Armis Inc. (or the Armis Affiliate with whom Customer has entered or is entering the Terms) ("**Armis**") and the Customer who purchased or is purchasing a subscription to either or both Intelligence Center and Early Warning ("**Customer**") subject to the Terms including this addendum available at https://www.armis.com/intelligence-center-early-warning-addendum/ unless the parties have entered another version of this Addendum in writing. Capitalized terms used but not defined in this Addendum shall have the meaning assigned to such terms in the Terms, and in case of a conflict among terms defined in the Addendum and terms defined in the Terms, this Addendum shall prevail.

1. Definitions.

1.1 "**Armis Data**" means the data, software code, or both, as obtained through the Product by Customer. Armis Data is Confidential Information as defined in the Subscription Terms.

1.2 "**Front End**" means the Armis-provided software solution that provides a graphical user interface that allows Authorized Users to interact with the Products through queries.

1.3 "**Product**" means the Intelligence Center or Early Warning product as subscribed to by Customer. The Product consists of (i) a database of potential security vulnerabilities in Customer's hardware environment and (ii) either or both (a) an API solution to enable Customer to access the Armis Data or (b) a Front End.

2. Use of the Products. Armis will make the Product (which includes the provision of Armis Data) listed in the Purchase Order available to Customer pursuant to the Terms and such Purchase Order. Except as otherwise stated in the Terms or Purchase Order, Customer shall have the non-exclusive, limited right to use the Product during the Subscription Period provided therein, unless earlier terminated in accordance with the Terms, solely for Customer's internal business purposes or as otherwise specified in the Purchase Order (the "**Purpose**").

3. Additional Restrictions. Notwithstanding anything to the contrary in the Terms, Customer may not, and may not cause or permit others to license, sell, transfer, assign, distribute, outsource, permit timesharing or service bureau use of, commercially exploit, or make available the Product, including the results or output of the Product, or any Armis Data obtained by or through the Product, to any Affiliate or third party. Customer shall not use the Product or Armis Data for any purpose other than the Purpose.

4. Data Security. Customer shall implement and maintain appropriate safeguards designed to protect the security, confidentiality, and integrity of Armis Data within its control. Customer shall without undue delay notify Armis if it becomes aware or reasonably suspects that any Armis Data has been subject to misappropriation, accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access that compromises the security, confidentiality or integrity of such information.

5. Warranties. Armis does not warrant or guarantee that the Product or Armis Data will facilitate the identification of every existing or potential risk or threat, result in error-free threat classification, or correct incident prioritization or risk assessment. Without limiting the foregoing, Armis provides the Product as an "as is" product without any warranties, express or implied, including, without limitation, warranties of merchantability, fitness for a particular purpose, accuracy, non-infringement, or those arising by law, statute, usage of trade, or course of dealing, and Armis' liability and liability limitations in connection with the Product shall be in accordance with its obligations under the Subscription Terms.

6. Requirements for Government Entities. If Customer is an agency or department of the United States federal government, then Customer shall only obtain the Armis Data through the Front End. The Product and Armis Data may not be shared with other agencies, foreign governments, or third-party contractors without explicit written authorization from Armis. Customer understands and agrees that DFARS 252.227-7013 and FAR 52.227-14 do not apply because the Product and Armis Data are commercial items under FAR 2.101.

ARMIS ON-PREM SUBSCRIPTION ADDENDUM TO

ARMIS PLATFORM TERMS AND CONDITIONS

This Armis On-Prem Subscription Addendum ("**Addendum**") to the Armis Platform Terms and Conditions ("**Terms,**" available at https://www.armis.com/legal-compliance/platform-terms-and-conditions/, unless another version of the Terms is entered into in writing among Armis and Customer (each, as defined below)) forms a part of the Terms between Armis Inc. (or the Armis Affiliate with whom Customer has entered or is entering the Terms) ("**Armis**") and the Customer who purchased or is purchasing a subscription to one or more Armis On-Prem Modules ("**Customer**") subject to the Terms including this addendum available at https://www.armis.com/legal-compliance/armis-on-prem-subscription-addendum/ unless the parties have entered another version of this Addendum in writing. Capitalized terms used but not defined in this Addendum shall have the meaning assigned to such terms in the Terms, and in case of a conflict among terms defined in the Addendum and terms defined in the Terms, this Addendum shall prevail.

References in the Terms to the Armis Platform (or corollary terms defining any Armis software subscribed to by Customer) apply to the Armis On-Prem Modules, as applicable. Customer agrees to be bound by this Addendum and the person acting on Customer's behalf hereby represents to Armis that they have the authority to bind Customer to this Addendum through consent or access to the Armis Solutions. If Customer does not agree to this Addendum or you do not have the authority to bind Customer to this Addendum, then Customer may not access to or use the Armis On-Prem Modules. The Parties agree as follows:

1. Definitions.

1.1. "**License Key**" means a unique string of alphanumeric characters that is used to activate, authenticate and use during the Subscription Term Customer's copy of any Armis On-Prem Module detailed in an applicable Purchase Order.

2. License.

2.1. **Access and Use.** During the Subscription Term, Armis grants Customer a limited, non-exclusive, non-assignable, revocable, non-sublicensable and non-transferable license to use one or more Armis On-Prem Module(s) as specified in one or more Purchase Orders, solely for Customer's internal business purposes, in accordance with the Terms and Documentation provided by Armis.

2.2. **License Restrictions.** In addition to any restrictions provided in the Terms, Customer and its Authorized Users shall not, and shall not authorize any third party to: (a) use any "open source copyleft software" in a manner that would require Armis to disclose the source code of the On-Prem Software to any third party; or (b) transmit any malicious code (i.e., software viruses, Trojan horses, worms, malware or other computer instructions, devices, or techniques that erase data or programming, infect, disrupt, damage, disable, or shut down a computer system or any component of such computer system) or other unlawful material in connection with its use of the On-Prem Module(s). Customer shall defend Armis against any claims, suits, actions, or proceedings brought against Armis and/or its directors, officers, and employees by a third party (including any regulatory authority) to the extent such claim arises from any such Customer's unauthorized use of the On-Prem Module.

3. Third-party Components. The Armis On-Prem Modules may use third-party open-source software, files, libraries, or components that may be distributed to Customer and are subject to third-party open-source license terms. If there is a conflict between any open-source license and the terms of this Addendum, then the open-source license terms shall prevail but solely in connection with the related third-party open-source software. Nothing in any open-source license limits Customer's rights to access and use the Armis On-Prem Module(s) as provided herein.

4. Intellectual Property. As between the parties, all right, title and interest (including, without limitation, all intellectual property rights) in the Armis On-Prem Module(s) are and shall be at all times, owned exclusively by Armis. This Addendum does not convey to Customer any interest in or to the Armis On-Prem Modules, other than the limited license expressly granted in Section 2 (License) above. Nothing herein constitutes a waiver of Armis's intellectual property rights under any law. Armis reserves all rights not expressly granted hereunder.

5. Delivery and Installation. Customer is responsible for installation of the Armis On-Prem Module(s) unless Customer has requested installation as Professional Services from Armis as detailed in an applicable Purchase Order. Armis will make the Armis On-Prem Module(s), License Key, and Documentation available to Customer for download from Armis's Support Portal or as may be agreed to by Customer and Armis in writing. Armis will provide reasonable assistance to Customer to enable Customer's access to and use of the Support Portal. During the Subscription Term, Customer shall have continued access to the Support Portal to download subsequent versions, updates and patches of the On-Prem Module(s) and related Documentation. Customer acknowledges that Armis has no other delivery obligations with respect to the On-Prem Module(s).

6. Continued Use. Customer's continued use of Armis On-Prem Modules is conditioned on Customer's continued

compliance with this Addendum and the Terms, and Customer's payment of all fees detailed in the relevant Purchase Order(s). Customer's License Key will be deactivated upon termination or expiration of the Subscription Term. Upon termination or expiration of this Addendum or the Terms, Customer shall delete and remove from all systems and storage media all copies of the Armis On-Prem Module(s), and shall certify in writing to Armis that it has complied with this requirement. If Customer continues to access or use the Armis On-Prem Module(s) anytime following the expiration of the Subscription Term, the terms and conditions of this Addendum and the Terms shall continue to apply, except Armis shall have no liability to Customer with respect to such use.

If the Parties are executing a signature version of this Addendum, the Parties' authorized representatives have agreed to and accepted these Terms as of the last date set forth below.

Customer:	_____	Armis:	_____
Signature:	_____	Signature:	_____
Name (Print):	_____	Name (Print):	_____
Title:	_____	Title:	_____
E-mail:	_____	E-mail:	Legal.notices@Armis.com
Date:	_____	Date:	_____