SOFTWARE AS A SERVICE LICENSE AGREEMENT

(v1-April-2024)

This Software as a Service License Agreement ("**SaaS Agreement**") is by and between the legal entity ("**Company**") as described in the applicable Quote (as defined below), as further defined below, and sets forth the terms, conditions, rights and restrictions for which Nagomi Security, Inc., a Delaware corporation with offices located at 488 Madison Ave, Floor 11, New York, NY 10022 United States, and any of its subsidiaries and affiliates (collectively or individually referred to as "**Vendor**") is willing to license its proprietary software ("**Software**") and to provide Professional Services (if agreed between the parties) (collectively referred to as "**Services**") to Company. Unless otherwise governed by a signed contract between Company and Vendor, this SaaS Agreement will apply to any Quotes made for the Services and Company's use thereof and such use is expressly contingent upon Company's acceptance of this SaaS Agreement, "AS IS". All additional and conflicting terms and conditions presented with or in any communication, including but not limited to those set forth in any P.O. (as defined below), except with respect to price, quantity, and location are hereby rejected, and shall be deemed *null* and *void*.

1. Definitions.

"Acceptable Use Policy" and/or "AUP" shall mean the set of rules and restrictions that Vendor may modify or update from time to time which set forth the proper way for Company to utilize Vendor's network and for permitted and appropriate use of the Software as a Service by Company, a copy of which is located at http://www.nagomisecurity.com/terms, which is hereby incorporated by reference.

"API(s)" shall mean the software application interfaces and workflow methods made generally available by Vendor to enable integration, implementation, and interoperability with third-party hardware and software.

"Data Protection Laws" shall mean applicable laws and regulations which seek to protect the processing and storage of personal information, including, but not limited to, the EU General Data Protection Regulation (GDPR) (EU 2016/679), the California Consumer Privacy Act.

"Documentation" shall mean any installation guides, reference guides, operation manuals and release notes provided with the Software in printed, electronic, or online form.

"Fees" shall mean the applicable fees due to Vendor, as detailed in a Quote, payable by Company in consideration for Vendor providing to Company the Software, Services, Maintenance & Support, and/or other license grants, set forth herein.

"Function(s)" shall mean additional features or usages of the Software for which Vendor may charge an additional fee.

"Go-Live Date" shall mean the first day that Vendor provides to Company access to utilize the Software as a Service for the Subscription Term.

"Personal Data" shall mean any information relating to an identified or identifiable natural person (hereafter a "**Data Subject**"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

"Professional Services" shall mean (i) configuration and installation services performed by Vendor's personnel and/or agents for the benefit of Company as reflected in an applicable Statement of Work(s) and/or Quote(s); (ii) SOWs; or (iii) per a pre-configured service package; and/or (iv) training services provided by Vendor's personnel and/or agents for the benefit of Company's personnel, agents or representatives.

"Maintenance & Support" &/or "M&S Services" shall mean those maintenance and support services provided to the Company as further set forth in the then-current Support Policy ("M&S Schedule"), a copy of which may be reviewed at .

"Purchase Order(s)" & "P.O.(s)" shall mean a purchaser order document, in tangible or intangible form (*e.g.* .rtf, .pdf, formats, etc.), issued by Company, indicating Company's acceptance of the reference Quote therein and this SaaS Agreement, without regards to any conflicting terms and conditions presented therein, except with respect to price, quantity, and location of Software or Services.

"Quote" shall mean the document under which Vendor offers for sale and licenses its Software, Services, and other services.

"Software as a Service" &/or "SaaS" shall mean the Software residing on a Vendor controlled network system servers, for which Company may access and utilize the Function(s) licensed herein and as further described in the applicable Quote.

"Software Development Kit" &/or "SDK" shall mean a set of software components, APIs, tools and Documentation that enables the Company to develop API(s) to allow for further interoperability with the Services.

"Statement of Work(s)" &/or "SOW(s)" shall mean the document(s), which detail Professional Services to be performed by Vendor, for the benefit of Company in furtherance of this Agreement, which references this Agreement and is signed by duly authorized representatives of the Parties.

"Subscription Term" shall mean the period of time commencing upon the Go-Live Date, which Company is entitled to utilize the SaaS, so long as Company has not lapsed in the payment of all applicable Subscription Services Fees due under any applicable Quotes.

"User(s)" shall mean an individual who is authorized by Company to utilize the Services.

2. License Grant & Restrictions. Subject to payment of the applicable Fees set forth in an applicable Quote, Vendor grants Company a limited, non-exclusive, non-transferable, revocable license to use the Software, as defined below, in conjunction with the Software solely for Company's internal business purposes in accordance with the Documentation for the Subscription Term.

2.1 Evaluation License. Should the applicable Quote indicate that the licenses granted therein are evaluation licenses, Vendor hereby grants Company a temporary, non-exclusive, non-transferable, revocable license to use the Software solely for internal testing, evaluation, proof-of-concept or demonstration purposes during the evaluation period set forth therein.

2.2 Pre-Released Software. Should the applicable Quote indicate that the licenses granted are for Software not yet commercially available ("Pre-Released Software"), then Vendor grants Company a temporary, non-exclusive, non-transferable, revocable license to use the Pre-Released Software and the associated Documentation, if any, as provided to Company by Vendor solely for internal evaluation purposes. Vendor may terminate Company's right to use the Pre-Released Software at any time at Vendor's sole discretion. Company's use of the Pre-Released Software is limited to thirty (30) calendar days unless otherwise set forth in the applicable Quote. Company acknowledges and agrees that (i) Vendor has not promised or guaranteed to Company that the Pre-Released Software will be announced or made available to anyone in the future; (ii) Vendor has no express or implied obligation to Company to announce or introduce the Pre-Released Software; (iii) Vendor may not introduce Software similar to or compatible with the Pre-Released Software; and (iv) any use of the Pre-Released Software or any Software associated with the Pre-Released Software is entirely at Company's own risk. During the term of this SaaS Agreement, if requested by Vendor, Company will provide feedback to Vendor regarding use of the Pre-Released Software. Company will not disclose any features or functions of any Pre-Released Software until Vendor makes the Pre-Released Software publicly available.

2.3 SDK License. Vendor grants Company a limited, non- exclusive, non-transferable revocable license to use the SDK, together with applicable documentation, any sample code, and any sample applications provided with the SDK, to create APIs solely in connection with Software for Company's internal business purposes.

2.4 Third-party Technology. The Software may contain embedded third-party technology ("Third-party Materials"). Third-party Materials are provided subject to the applicable third-party terms of use; and Company hereby agrees to abide by the third-party terms of use and/or to obtain any additional licenses that may be required to use the Third-party Materials. Vendor makes no warranty or indemnity hereunder with respect to any Third-party Materials. The term "Services" shall include the said Third-party Materials.

2.5 License Restrictions. Company specifically agrees to limit the use of the Software, Documentation, and Third-party Materials to those specifically granted in this SaaS Agreement for the Subscription Term as set forth herein and in the applicable Quote. Without limiting the foregoing, Company specifically agrees not to (i) attempt to reverse engineer, decompile, disassemble, or attempt to derive the source code of the Software or any portion thereof; (ii) modify, port, translate, localize or create derivative works of the Software and/or Third-party Materials; (iii) remove any of Vendor's or its vendors' copyright notices and proprietary legends; (iv) attempt to circumvent, disable or defeat the limitations on Vendor's use of the Software, which are encoded into the Software and/or Third-party Materials; (v) use the Software and/or Third-party Materials (a) to infringe on the intellectual property rights of any third party or any rights of publicity or privacy; (b) to violate any law, statute, ordinance or regulation (including but not limited to the laws and regulations governing export/import control, unfair competition, anti-discrimination and/or false advertising); (c) to propagate any virus, worms, Trojan horses or other programming routine intended to damage any system or data; and/or (d) such that the total number of Users used, the Functions licensed, and IDs issued are in excess of the total number allocated to Company, as reflected in the applicable Quote; (vi) file copyright or patent applications that include the Software and/or Third- party Materials or any portion thereof; (vii) use the Third-party Materials within any other applications or products other than with the Software; (viii) sell, assign, transfer, lease, rent, sublicense, or otherwise distribute or make available the Services to any third party (such as offering it as part of a time-sharing, outsourcing or service bureau environment), and/or make any use or otherwise exploit the Services for commercial or business use; (ix) publicly perform, display or communicate the Services; (x) alter, adapt, arrange, or translate the Services; (xi) use any "open source" or "copyleft software" in a manner that would require Vendor to disclose the source code of the Software or other provided Services to any third party; and/or (xii) disclose the results of any testing or benchmarking of the Services and/or the contents of the Services to any third party. Company and/or any User shall immediately report any unauthorized access or use of the Services (or any other activity with respect to their accounts) or breach of these restrictions by a User or any third party to Vendor. Vendor reserves the right to terminate this Agreement for cause in case Company materially breaches the provisions of this Section.

2.6 License & IP Audit Rights. Company agrees to maintain records reasonably required to verify its compliance with this SaaS Agreement, including but not limited to Company's compliance with the restriction set forth in Section 2.5 "License Restrictions". Within fifteen (15) calendar days of receipt of a written request, Company shall either (i) provide a certified report indicating the number of Users being utilized; (ii) conduct a webinar to show Vendor the number of Users being utilized; or (iii) allow Vendor to remotely access the Company's controlled network system servers. In the event that Vendor determines that Company has over deployed the Software such that it is utilizing more Users then licensed hereunder, Vendor shall notify Company in writing of any alleged discrepancy and Company agrees to pay such amounts within thirty (30) calendar days from receipt of such notification. The amount due shall be calculated from the initial time of over deployment and shall be subject to interest at the lesser of one and a half (1.5 %) percent per month or the highest rate permitted by law.

3. Intellectual Property Rights & Protection.

3.1 Intellectual Property Rights. Vendor retains all rights, title and interest in and to the Software and Services. In all instances, Vendor retains all rights, title, and interest, including, but not limited to, all intellectual property rights such as copyright, patent, trademark, service mark, trade secret, and *suis generis* rights in and to the Software, SDK, and Third-party Materials, and all copies thereof including all derivations, modifications and enhancements thereto. This Agreement does not provide Company with title or ownership of the Software, SDK, and Third-party Materials, but only a right of limited use as outlined herein. Company (and shall ensure that the Users, as well as other employees and staff of Company) shall make, and hereby irrevocably make, all necessary assignments or assignments reasonably requested by Vendor to ensure and/or provide Vendor with the ownership rights set forth in this paragraph. Nothing herein constitutes a waiver of Vendor's intellectual property rights under any law.

3.2 Feedback. If Vendor receives any feedback (which may consist of questions, comments, suggestions or the like) regarding any of the Services (collectively, "**Feedback**"), all rights, including intellectual property rights in such Feedback shall belong exclusively to Vendor and such shall be considered Vendor's Confidential Information. Company hereby irrevocably and unconditionally transfers and assigns to Vendor (and shall ensure that each User irrevocably and unconditionally transfers and assigns) all intellectual property rights it has in such Feedback and waives any and all moral rights that Company may have in respect thereto. It is further understood that use of Feedback, if any, may be made by Vendor at its sole discretion, and that Vendor in no way shall be obliged to make use of the Feedback.

3.3 Analytic Information. Any anonymous information, which is derived from the use of the Services (i.e., metadata, aggregated and/or analytics information and/or intelligence relating to the operation, support, and/or Company's use, of the Service) which is not personally identifiable information ("**Analytics Information**") may be used for providing the Services, for development, and/or for statistical purposes. It is specifically acknowledged and agreed between the Parties that that no compensation, whatsoever, is nor shall be due to Company for any such information or use thereof. Such Analytics Information is Vendor's sole and exclusive property.

4. Acceptable Use Policy & Operational Concerns.

4.1 Appropriate Use of the SaaS. While Services may be used by the appropriate User(s) that Company authorizes, Company may not sublicense, resell or supply the Service for use in or for the benefit of any other organization, entity, business, or enterprise without Vendor's prior written consent. Company agrees not to submit to the SaaS any material that is illegal, misleading, defamatory, indecent or obscene, in poor taste, threatening, infringing of any third-party proprietary rights, invasive of personal privacy, otherwise objectionable or in violation of Vendor's AUP (collectively "**Objectionable Matter**"). Company will be responsible to ensure that the Users do not submit any Objectionable Matter. In addition, Vendor reserves the right to remove any data that constitutes Objectionable Matter or violates any Vendor rules regarding appropriate use or AUP but is not obligated to do so. Company and Users will comply with all applicable laws regarding Company's Data, use of the Service and the Software, including laws involving personal data and any applicable export controls. Vendor reserves the right to terminate this Agreement for cause in case Company materially breaches the provisions of this Section.

4.2 Certificate Security. Company is responsible for maintaining the security and confidentiality of all certificates, usernames, identification numbers, and access keys. Company shall not disclose or make available such certificates, usernames, identification numbers, and access keys other than to Company authorized employees and shall use best efforts to prevent unauthorized access to, or use of, the Services. In the event that Company makes such certificates, usernames, identification numbers, and access keys available to any third-party, as between Vendor, its suppliers and Company, Company shall be solely liable for all actions taken by such third-party and resulting consequences. Company agrees to notify Vendor immediately of any unauthorized use, loss or theft of any such certificates, usernames, identification numbers, and access keys, or any other known or suspected breach of security.

4.3 Termination or Suspension of Services. Vendor reserves the right to suspend or terminate, immediately without notification, any of Company's or an individual user's access to the Services that, which in Vendor's reasonable opinion, (i) is or has the potential of disrupting or causing harm to Vendor's or any third-party's computers, networks, systems or infrastructure; (ii) is in violation of the Vendor AUP; (iii) is in violation of state, federal and/or international laws/policies regarding "spam," including, without limitation, the CAN-SPAM Act of 2003; (iv) is in violation of state, federal and/or international laws/policies regarding data protection including, without limitation, the Data Protection Laws; (v) the use of Services adversely effects Vendor's or its suppliers' equipment, security network infrastructure, or service(s) to others; (vi) a court or other governmental authority having jurisdiction issues an order prohibiting Vendor from furnishing the Services to Company; or (vii) Company fails to pay undisputed charges for the Services after being given notice; provided Fees will continue to accrue for Company's Data notwithstanding any suspension and Company will remain liable for all Fees; and/or (viii) violates Section 2 "License Grant & Restrictions" or Section 4 "Acceptable Use Policy & Operational Concerns".

5. Warranties.

5.1. Software Warranty. Vendor warrants, for Company's benefit alone, that the Software will conform materially and substantially to the Documentation during the Subscription Term ("Software Warranty"), as set forth in the applicable Quotes.

5.2 Professional Services Warranty. Vendor warrants that all Professional Services shall be performed in a professional and workmanlike manner, consistent with then-current industry standards ("Professional Services Warranty"). Company's sole and exclusive remedy for a breach of the Professional Services Warranty shall be, at Vendor's option, either to (i) re-perform such Professional Services; or (ii) to provide Company with a refund for the allegedly defective Professional Services. Such remedy shall only be available if Company notifies Vendor in writing within thirty (30) calendar days of the completions of each individual deliverable as set forth in the applicable Statement of Work.

5.3 Warranty Exclusions. The foregoing warranties set forth herein do not apply to any failure of the Software or Services caused by (a) Company's failure to follow Vendor's installation, operation, or Services instructions, procedures, or Documentation; (b) Company's mishandling, misuse, negligence, or improper installation, de-installation, storage, servicing, or operation of the Software; (c) modifications or repairs not authorized by Vendor; (d) use of the Software in combination with equipment or software not supplied by Vendor or authorized in the Documentation; and/or (e) power failures or surges, fire, flood, accident, actions of third parties, or other events outside Vendor's reasonable control. Vendor cannot and does not warrant the performance or results that may be obtained by using the Software, nor does Vendor warrant that the Software are appropriate for Company's purposes or error-free. If during the Software Warranty Period, a nonconformity is reported to Vendor, Vendor, at its option, will use commercially reasonable efforts to repair or replace the non-conforming Software. THE REMEDIES STATED IN THIS SECTION 5, "WARRANTIES", ARE COMPANY'S SOLE AND EXCLUSIVE REMEDY, AND VENDOR'S SOLE LIABILITY FOR A BREACH OF WARRANTY. EXCEPT FOR THE EXPRESS WARRANTIES STATED IN THIS SECTION 5, "WARRANTIES", VENDOR DISCLAIMS ALL WARRANTIES ON MERCHANDISE SUPPLIED UNDER THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

6. Maintenance & Support Services. So long as Company has not lapsed in its payment of Subscription Service Fees due hereunder during the Subscription Term, Vendor shall provide Company (i) support services as further described in then-current M&S Schedule, a copy of which may be reviewed at http://www.nagomisecurity.com/terms; (ii) all upgrades and updates,

at no additional charge ((i) and (ii) may individually or collectively be referred to as "M&S Services"). It is the responsibility of Company to obtain and install all upgrades and updates. Vendor reserves the right to withhold M&S Services if Company (i) has lapsed in payment of the applicable Subscription Fees; (ii) failed to update the Software.

7. Prices, Payments & Taxes.

7.1 Prices. The prices for the Services are set forth in the applicable Quote(s); however, the prices for Professional Services Fees might be set forth in Statements of Work(s) and/or Quote(s). All Fees are exclusive of sales, use, value-added or other excise tax, however designated or levied, and therefore are subject to an increase in an amount equal to any tax Vendor may be required to collect or pay (excluding taxes on its income). Company acknowledges and agrees that all prepaid Fees are non-refundable and no credits shall be made except as provided for in Section 5, "Warranties".

7.2 Payment. All invoices shall be due and payable within thirty (30) calendar days after invoice date. Unless otherwise specified in the applicable Quote all amounts due are in U.S. Dollars. Vendor may impose late charges on overdue payments at a rate equal to the lesser of one and a half (1.5%) percent per month or the highest rate legally permitted by law, calculated from the date payment was due until the date payment is made and all expenses incurred in collection, including reasonable attorneys' fees. For all versions of the Services, Vendor reserves the right in the future to charge a fee for features and/or uses which are currently made available free of charge or may be made available to Company in the future, provided that Vendor gives Company at least thirty (30) days' notice of such changes.

7.3 Taxes. Company shall be liable for payment of all local state and federal sales, use, excise, personal property or other similar taxes or duties that are levied upon and related to the performance of obligations or exercise of rights under this Agreement. Vendor may be required to collect and remit taxes from Company, unless Company provides Vendor with a valid tax exemption certificate. Vendor will invoice Company for all such taxes based on Software and/or Services provided hereunder. In no event will either party be responsible for any taxes levied against the other party's net income.

8. Confidential Information & Data Rights.

8.1 Confidential Information. "**Confidential Information**" shall mean any and all non-public technical, financial, commercial or other confidential or proprietary information, Services, roadmaps, pricing, software code, Documentation, techniques and systems, and any and all results of benchmark testing run on the Software. Neither party will disclose Confidential Information to any third party except to the extent such disclosure is necessary for performance of this SaaS Agreement, or it can be documented that any such Confidential Information is in the public domain and generally available to the general public without any restriction, or to the extent disclosure is expressly required by applicable law. Each party will use the same degree of care to protect Confidential Information as Company uses to protect Company's own confidential information but in no event less than reasonable care. Confidential Information does not include any information which: (i) is or becomes generally known and available to the public through no act of the recipient; (ii) was already in the recipient's possession without a duty of confidentiality owed to the discloser at the time of the discloser's disclosure; (iii) is lawfully obtained by the recipient from a third party who has the express right to make such disclosure; or (iv) is independently developed by the recipient without breach of an obligation owed to the discloser. The recipient may use the discloser's Confidential Information solely to perform its obligations under this SaaS Agreement.

8.2 Data Usage Rights. During the Subscription Term, Company may provide to Vendor certain data about Company's use of the Software ("**Company Data**"). Vendor may use such Company Data in connection with the performance of its obligations under this SaaS Agreement. The Company shall be solely responsible for making backup copies of Company Data and is solely liable for the completeness, integrity, quality and accuracy of Company Data. To the extent Company processes personal information through the Services, this Agreement incorporates the Vendor's Data Processing Agreement located at http://www.nagomisecurity.com/terms ("**DPA**"), which shall govern such processing activities.

8.4. Reference Customer. Company agrees that Vendor may identify Company as a user of the Services and use Company's trademarks and/or logo (i) in its sales presentations, promotional/marketing materials, and press releases, and (ii) in order to develop a brief customer profile for use by Vendor on its website and other promotional channels for promotional purposes.

9. Term & Termination.

The term of this SaaS Agreement shall be for the duration of the Subscription Term as set forth in the applicable Quote. During Subscription Term either party may terminate this SaaS Agreement, immediately, upon providing written notice of material breach to the other party, if such other party fails to cure such materially breaches within a period of thirty (30) calendar days following receipt of such written notice. Upon any termination of this SaaS Agreement, (i) all licenses granted hereunder shall immediately terminate, (ii) Company will either return the Software and Documentation and any other part of the Services, or with Vendor's prior written consent, destroy the Software and Documentation and any other part of the Services.

10. LIMITATION OF LIABILITY & EXCLUSION OF CONSEQUENTIAL DAMAGES.

10.1 LIMITATION OF LIABILITY. NOTWITHSTANDING ANYTHING TO THE CONTRARTY AND TO THE EXTENT PERMITTED BY LAW, VENDOR (ITS AFFILIATES, OUR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, AND AGENTS OR ANY LICENSOR OR SUPPLIER) SHALL NOT BE LIABLE FOR ANY LOSS OR DAMAGE UNLESS SUCH LOSS OR DAMAGE IS DUE TO VENDOR'S NEGLIGENCE AND/OR WILLFUL MISCONDUCT. IF VENDOR IS FOUND LIABLE, THE AMOUNT OF VENDOR'S MAXIMUM LIABILITY FOR ANY AND ALL LOSSES AND/OR DAMAGES (IN CONTRACT, TORT, OR OTHERWISE) SHALL NOT EXCEED THE TOTAL AMOUNT OF ALL FEES ACTUALLY PAID TO VENDOR S WITHIN THE PRIOR SIX (6) MONTHS FROM WHICH SUCH CLAIM ARISES.

10.2 EXCLUSION OF CONSEQUENTIAL DAMAGES. NOTWITHSTANDING ANYTHING TO THE CONTRARTY, AND TO THE EXTENT PERMITTED BY LAW, EXCEPT FOR FRAUD OR GROSS NEGLIGENCE, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, PUNITIVE, AND/OR INCIDENTAL DAMAGES, WHATSOEVER, INCLUDING, BUT NOT LIMITED

TO ,LOST PROFITS OR LOSS OF DATA, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH POTENTIAL LOSS OR DAMAGE.

10.3 ESSENTIAL PURPOSE. THE LIMITATION OF LIABILITY AND EXCLUSION OF CERTAIN DAMAGES STATED HEREIN SHALL APPLY REGARDLESS OF THE FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY. BOTH PARTIES HEREUNDER SPECIFICALLY ACKNOWLEDGE THAT THESE LIMITATIONS OF LIABILITY ARE REFLECTED IN THE PRICING.

11. Indemnification. For any claims based on Company's breach of Sections titled, "License Grant and Restrictions", "Confidential Information & Data Usage Rights", "Compliance & Export Controls", and/or Company use of Software, the Services, Company hereby agrees to indemnify, defend, and hold Vendor harmless against such claim(s) at Company's expense and pay all damages that a court of competent jurisdiction finally awards, provided that Vendor(i) promptly notifies Company in writing of the claim(s); (ii) allows Company to control the defense or any related settlement negotiations; and (iii) cooperates with Company in the defense of any such claim(s); provided, that, Company will not affect any settlement unless such settlement provides Vendor with a full release.

12. Compliance & Export Controls. Company shall comply fully with all applicable laws, rules, and regulations including. But not limited to those of the United States, and any and all other jurisdictions globally, which apply to Company's business activities in connection with this SaaS Agreement. Company acknowledges that the Vendor Software and/or Vendor Services are subject, amongst others, to United States Government export control laws. Company shall comply with all applicable export control laws, obtain all applicable export licenses, and will not export or re-export any part of the Software and/or Services to any country in violation of such restrictions or any country that may be subject to an embargo by the United States Government or to End-Users owned by, or with affiliation to, such countries embargoed by the United States Government.

13. U.S. Government Use Notice. The Software is a "Commercial Item", as that term is defined at 48 C.F.R. § 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. § 12.212 and 48 C.F.R. § 227.7202, as applicable. Consistent with 48 C.F.R. § 12.212 and 48 C.F.R. § 227.7202-1 through 227.7202-4, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government End-Users (a) only as Commercial Items and (b) with only those rights as are granted to all other End-Users pursuant to the terms and conditions herein. For some components of the Software as specified in the Exhibit, Attachment, and/or Schedule, this Software and Documentation are provided on a RESTRICTED basis. Use, duplication, or disclosure by the United States Government is subject to restrictions set forth in Subparagraphs (c) (1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable.

14. Relationship Between the Parties. The relationship between the parties established by this SaaS Agreement is that of independent contractors, and nothing contained in this SaaS Agreement shall be construed to: (i) give either party the power to direct or control the day-to-day activities of the other; (ii) constitute the parties as partners, joint ventures, co-owners or otherwise as participants in a joint or common undertaking or franchise; (iii) allow Company to create or assume any obligation on behalf of Vendor for any purpose whatsoever; or (iv) allow any Company, User, or other person or entity not a party to this SaaS Agreement to be considered a third-party beneficiary of this SaaS Agreement.

15. General Provisions.

15.1 Entire Agreement T&Cs & Integration. This SaaS Agreement and all Exhibits referencing this SaaS Agreement represent the entire agreement between the parties on the subject matter hereof and supersede all prior discussions, agreements and understandings of every kind and nature between the parties. Neither party shall be deemed the drafter of this SaaS Agreement. No modification of this SaaS Agreement shall be effective unless in writing and signed by both parties. All additional and conflicting terms and conditions presented with or in any communication, including but not limited to Company's P.O., except with respect to price, quantity, and location specified in a P.O., are hereby rejected, and shall be deemed null and void.

15.2 Severability & Survival. The illegality or unenforceability of any provision of this SaaS Agreement shall not affect the validity and enforceability of any legal and enforceable provisions hereof. Should any provision of this SaaS Agreement be deemed unenforceable by a court of competent jurisdiction then such clause shall be re-construed to provide the maximum protection afforded by law in accordance with the intent of the applicable provision. Any provision contained herein, which by its nature should survive the termination of this SaaS Agreement shall survive, including, but not limited to, the Section titled "License Restrictions",
"Intellectual Property Rights & Protection", "Confidential Information & Data Usage Rights", "Limitation of Liability & Exclusion of Consequential Damages", "Indemnification", "Compliance & Export Controls", and "General Provisions".

15.3 Assignment. Neither party may assign any rights or delegate any obligations hereunder without the other Party's consent, which consent will not be unreasonably withheld. Each Party will be entitled to assign its rights and obligations arising from this SaaS Agreement in whole or in part without restrictions of any kind due to a consolidation or merger of such Party with or into, or a sale of all or substantially all of such Party's assets to, or substantially all of such Party's issued and outstanding share capital to, such other entity. This SaaS Agreement bindS the parties, their respective participating subsidiaries, affiliates, successors, and permitted assigns.

15.4 Applicable Law & Disputes. The parties specifically agree that the U.N. Convention on the International Sale of Goods, the Uniform Computer Information Transactions Act (UCITA), shall not apply to any and all actions performed by either party hereunder in furtherance of this SaaS Agreement. This SaaS Agreement and all resulting claims and/or counterclaims shall be governed, construed, enforced and performed in accordance with the laws of the State of New York, United States of America, without reference and/or regard to its conflicts of laws principles. Any such dispute arising out of or in connection or associated with this SaaS Agreement shall be referred to and finally resolved by arbitration, by a single arbitrator, in accordance with the Rules of the American Arbitration Association then in force ("Arbitration"); provided, however, that either party may, at its sole discretion, seek injunctive relief in the courts of any jurisdiction as may be necessary and appropriate to protect its proprietary or confidential information. The language used in the arbitral proceedings, and the governing language of this SaaS Agreement, shall be English. Unless otherwise mutually agreed upon in writing by the parties, the site of the Arbitration shall be in New York City, New York, U.S.A. Judgment upon the award of the arbitration may be entered in any court having jurisdiction thereof.

15.5 Force Majeure. Neither party shall be liable for any failure or delay in performing Services or any other obligation under this SaaS Agreement, nor for any damages suffered by the other or an end-user by reason of such failure or delay, which is, indirectly or directly, caused by an event beyond such party's foreseeable control including but not limited to strikes, riots, natural catastrophes, terrorist acts, pandemic, governmental intervention, or other acts of God, or any other causes beyond such party's reasonable control.

15.6 Waiver. Each party agrees that the failure of the other party at any time to require performance by such party of any of the provisions herein shall not operate as a waiver of the rights of such party to request strict performance of the same or like provisions, or any other provisions hereof, at a later time.

15.7 Notices. All notices under this SaaS Agreement shall be in English and shall be in writing and may be sent to a party's headquarters labelled "Attn: Legal", either by (i) registered airmail; (ii) overnight delivery through a reputable third-party courier; or (iii) *via* electronic mail (email) sent "read receipt" and "delivery receipt". With respect to Vendor's receipt of electronic notice set forth in (iii) above such notice shall only been deemed received once Company receives a confirmation of "read receipt" and "delivery receipt" and such notice shall only be valid if sent to legal@nagomisecurity.com.

***

Nagomi Security Customer Support Policy

(v1-April-2024)

Nagomi Security, Inc. ("Vendor") provides support to assist our customers with the use of the Vendor products and services. Vendor is committed to providing world-class support and will undertake all due efforts, in accordance with then-current industry standards and best practices, in order to respond to support requests in accordance with the time-frames defined in the applicable Customer Support Plan, ("Support Service(s)") as further described below.

Access to Vendor's Customer Support services are submitted and tracked *via* an online ticketing system. Requests for support services ("Support Request(s)") may be submitted either *via* (i) a web form at our support site located at https://support.nagomisecurity.com ("Support Portal"); or (ii) email at support@security.com . Further the Support Portal contains community support, product documentation, and knowledge base documentation.

Scope

Eligibility

To receive Support Services from Vendor the customer must have an up-to-date, paid and valid subscription for such Support Service.

Responsibilities

Vendor shall:

- Provide access to all generally available updates, upgrades, enhancements, fixes and new versions of the software; and
- Provide customers with online access to a Support Portal. The support portal may include a ticket submission system, ticket statuses and history, knowledge articles and product documentation.

Customer shall:

- Provide prompt notice of any issue *via* the Support Portal;
- Provide a detailed description of the issue(s);
- Provide promptly any additional information requested, targeted to, but not limited to reproducing the issue(s);
- Cooperate and show good will in assisting with the investigation into the issues; and
- Assign primary contacts who are expected to work with Vendor's Support staff in order to solve the reported issue(s).

Service Availability

The Support Services provided by Vendor are targeted to maintain a 99.9% uptime per calendar month. The availability of such Support Services does not include regularly scheduled maintenance, downtime that results from third-party interference or which are Vendor's reasonable control, which includes but is not limited to the following:

- An initial misconfiguration;
- A customer cause;
- An update to configuration that the customer has been asked to perform in advance but for which was not performed; or
- Failure of the Customer Internet service provider(s).

Limitations

Vendor's obligation to provide Support Services shall apply only to the supported releases per Vendor's end-of-life policy. Any custom development done by a third-party, customer or Vendor is outside of the scope of this policy, unless explicitly agreed in a separate contract. Email submissions of tickets are treated as an information request until investigated.

Response Time

The response time is measured from the time Vendor receives the Support Request until Vendor has responded to that Support Request. Vendor does not guarantee resolution times, and a resolution may consist of a fix, workaround, service availability, or other solution what Vendor deems reasonable.

Priority Levels

A Support Request by a customer will be classified in one of four priority levels. The priority level along with the support plan will define the response times, including response-times and update frequency.

Classification	Definition
Priority 1	An issue that prevents operation of critical documented functions with high frequency or duration. Essentially unable to use the product and widespread issue. Priority 1 issues require the customer to have dedicated resources available to work on the issue on an ongoing basis with Vendor.
Priority 2	An issue that consistently prevents operation of non-critical documented functions or occasionally impacts critical documented functions or a critical issue for which a temporary work around has been provided.
Priority 3	An issue that has some impact on administration, non-critical operation or other secondary functions or a major issue for which a temporary work around has been provided.
Priority 4	The services are unaffected; Customer requests product related technical advice or general information and feature questions related to the products.

Priority 1 Cases

Vendor will provide continuous efforts (24/7/365) to resolve Priority 1 Support Requests, until a workaround or resolution can be provided or until the issue can be downgraded to a lower severity.

Upgrade/Downgrade of Priority Level

If, during the Support Request process, the issue either (i) requires assignment of a higher priority level than currently assigned; or (ii) no longer requires the priority level currently assigned, based on its current impact to the product or services, then the priority level will be upgraded or downgraded accordingly to the priority level that most appropriately reflects the current impact.

Support Plans

Vendor’s Premium Customer Support Plan is included in all Vendor subscriptions.

Premium Plan
Enterprise Support 24x7
Premium Plan Performance Metrics

Community Support
Web Portal
Email ticket creation
Level 2 (Pool)

Vendor will undertake all due efforts in order to respond to Support Requests, in accordance with then-current industry standards and best practices, and endeavors to respond in a manner consistent with the time-frames defined in the selected Customer Support Plan. All time-frames defined in the applicable Customer Support Plan are only available and calculated during and within such Customer Support Plan's business support hours, as set forth below.

Premium Plan Performance Metrics

Classification	Time to First Response	Update Frequency
Priority 1	Acknowledgment within (1) hours of Customer's submission of support request.	(2) hours
Priority 2	Acknowledgment within (2) hours of Customer's submission of support request	(4) hours
Priority 3	Acknowledgment within (4) hours of Customer's submission of support request	(8) hours
Priority 4	Acknowledgment within (8) hours of Customer's submission of support request	(8) hours

Business Support Hours: 24 hours a day, 7 days a week, 365 days a year

{End}
***

DATA PROCESSING AGREEMENT/ADDENDUM

This Data Processing Agreement ("**DPA**") is made and entered into as of the execution date and forms part of the Nagomi Security, Inc. Agreement (the "**Agreement**"). You acknowledge that you, as the customer identified in the execution signature and/or the Agreement (collectively, **"You", "Your", "Customer", or "Data Controller"**) have read and understood and agree to comply with this DPA, and are entering into a binding legal agreement with Nagomi Security Inc. as defined below (**"Nagomi"**, **"Us"**, **"We", "Our", "Service Provider" or "Data Processor"**) to reflect the parties' agreement with regard to the Processing of Personal Data (as such terms are defined below). Both parties shall be referred to as the "**Parties**" and each, a "**Party**".

WHEREAS, Nagomi shall provide the services set forth in the Agreement (collectively, the "**Services**") for Customer, as described in the Agreement; and

WHEREAS, In the course of providing the Services pursuant to the Agreement, we may process Personal Data on your behalf, in the capacity of a "**Data Processor**"; and the Parties wish to set forth the arrangements concerning the processing of Personal Data (defined below) within the context of the Services and agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

NOW THEREFORE, in consideration of the mutual promises set forth herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Parties, the parties, intending to be legally bound, agree as follows:

1. INTERPRETATION AND DEFINITIONS

1.1 The headings contained in this DPA are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this DPA. References to clauses or sections are references to the clauses or sections of this DPA unless otherwise stated. Words used in the singular include the plural and vice versa, as the context may require. Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement. Definitions:

(a) "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "**Control**", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

(b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws And Regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Nagomi, but has not signed its own agreement with Nagomi and is not a "**Customer**" as defined under the Agreement.

(c) "**Controller**" or "**Data Controller**" means the entity which determines the purposes and means of the Processing of Personal Data. For the purposes of this DPA only, and except where indicated otherwise, the term "Data Controller" shall include the Organization and/or the Organization's Authorized Affiliates.

(d) "**CCPA**" means the California Consumer Privacy Act of 2018 and its modifications and amendments.

(e) "**Data Protection Laws and Regulations**" means all laws and regulations of the European Union, the European Economic Area and their Member States, including the GDPR, the UK GDPR, and the Israeli Privacy Protection Law, 1981 and the regulations promulgated thereunder (including Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761-2001 and Privacy Protection Regulations (Data Security), 5777-2017), and any binding instructions, guidelines and requirements of the Israeli Privacy Protection Authority, as applicable to the Processing of Personal Data under the Agreement.

(f) "**Data Subject**" means the identified or identifiable person to whom the Personal Data relates.

(g) "**Member State**" means a country that belongs to the European Union and/or the European Economic Area. "**Union**" means the European Union.

(h) "**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(i) "**Personal Data**" or "**Personal Information**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, as defined under Data Protection Laws and Regulations and/or under the CCPA, as applicable. For the avoidance of doubt, Customer's business contact information is not by itself deemed to be Personal Data subject to this DPA.

(j) "**Process(ing)**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

(k) "**Processor**" or "**Data Processor**" means the entity which Processes Personal Data on behalf of the Controller.

(l) "**Security Documentation**" means the Security Documentation applicable to the specific Services purchased by Customer, as updated from time to time. The current version is available on Schedule 4 herein.

(m) **"Standard Contractual Clauses" or "SCCs"** means (i) the standard contractual clauses for the transfer of Personal Data to Data processors established in third countries which do not ensure an adequate level of protection as set out in Regulation (EU) 2016/679 of the European Parliament and of the Council from June 4, 2021, as available here as updated, amended, replaced or superseded from time to time by the European Commission; or (ii) where required from time to time by a supervisory authority for use with respect to any specific restricted transfer, any other set of contractual clauses or other similar mechanism approved by such Supervisory Authority or by Applicable Laws for use in respect of such Restricted Transfer, as updated, amended, replaced or superseded from time to time by such Regulatory Authority or Data Protection Laws and Regulations**;**

(n) “**Sub-processor**” means any Processor engaged by Nagomi and/or Nagomi Affiliate to Process Personal Data on behalf of Customer;

(o) “**Supervisory Authority**” means an independent public authority which is established by an EU Member State pursuant to the GDPR;

(p) “**UK GDPR**” means the Data Protection Act 2018, as updated, amended, replaced or superseded from time to time by the ICO;

(q) **“UK Standard Contractual Clauses” or “UK SCCs”** means the standard contractual clauses for the transfer of Personal Data to Data processors established in third countries which do not ensure an adequate level of protection as set out by the ICO, as available here, as updated, amended, replaced or superseded from time to time by the ICO;

(r) “**Nagomi**” means the relevant Nagomi entity of the following Nagomi legal entities as specified in this DPA and/or in the Agreement, including: Nagomi Security, Inc.; and Nagomi Security Ltd.

(s) “**Nagomi Group**” means Nagomi and its Affiliates engaged in the Processing of Personal Data.

2. PROCESSING OF PERSONAL DATA

2.1 The Parties acknowledge and agree that with regard to the Processing of Personal Data under this DPA Nagomi is the Data Processor and Nagomi or members of the Nagomi Group may engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” below. For clarity, this DPA shall not apply with respect to Nagomi processing activity as a Data Controller as detailed in Nagomi’s privacy policy.

2.2 Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations and comply at all times with the obligations applicable to data controllers (including, without limitation, Article 24 of the GDPR). For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the means by which Customer acquired Personal Data. Without limitation, Customer shall comply with any and all transparency-related obligations (including, without limitation, displaying any and all relevant and required privacy notices or policies) and shall at all times have any and all required ongoing legal bases in order to collect, Process and transfer to Nagomi the Personal Data and to authorize the Processing by Nagomi of the Personal Data which is authorized in this DPA.

2.3 Nagomi’s Processing of Personal Data.

2.3.1 Subject to the Agreement, Nagomi shall Process Personal Data that is subject to this DPA only in accordance with Customer’s documented instructions as necessary for the performance of the Services and for the performance of the Agreement and this DPA, unless required to otherwise by Union or Member State law or any other applicable law to which Nagomi and its Affiliates are subject, in which case, Nagomi shall inform the Customer of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The duration of the Processing, the nature and purposes of the Processing, as well as the types of Personal Data Processed and categories of Data Subjects under this DPA are further specified in **Schedule 1** (Details of the Processing) to this DPA.

2.3.2 To the extent that Nagomi or its Affiliates cannot comply with a request (including, without limitation, any instruction, direction, code of conduct, certification, or change of any kind) from Customer and/or its authorized users relating to Processing of Personal Data or where Nagomi considers such a request to be unlawful, Nagomi (i) shall inform Customer, providing relevant details of the problem (but not legal advice), (ii) Nagomi may, without any kind of liability towards Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing those data), and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, each Party may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Customer shall pay to Nagomi all the amounts owed to Nagomi or due before the date of termination. Customer will have no further claims against Nagomi (including, without limitation, requesting refunds for Services) due to the termination of the Agreement and/or the DPA in the situation described in this paragraph (excluding the obligations relating to the termination of this DPA set forth below).

3. **RIGHTS OF DATA SUBJECTS.** If Nagomi receives a request from a Data Subject to exercise its rights as laid down in Chapter III of the GDPR (“**Data Subject Request**”), Nagomi shall, to the extent legally permitted, promptly notify and forward such Data Subject Request to Customer. Taking into account the nature of the Processing, Nagomi shall use commercially reasonable efforts to assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

4. NAGOMI PERSONNEL

4.1 Nagomi shall grant access to the Personal Data to persons under its authority (including, without limitation, its personnel) only on a need-to-know basis and ensure that such persons engaged in the Processing of Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.2 Nagomi may disclose and Process the Personal Data (a) as permitted hereunder (b) to the extent required by a court of competent jurisdiction or other Supervisory Authority and/or otherwise as required by applicable laws or applicable Data Protection Laws and Regulations (in such a case, Nagomi shall inform the Customer of the legal requirement before the disclosure, unless that law prohibits such information on important grounds of public interest), or (c) on a "need-to-know" basis under an obligation of confidentiality to legal counsel(s), data protection advisor(s), accountant(s), investors or potential acquirers.

5. AUTHORIZATION REGARDING SUB-PROCESSORS

5.1 Nagomi's current list of Sub-processors is included in **Schedule 2** ("**Sub-processor List**") and is hereby approved by Data Controller. Customer hereby grants a general authorization to Nagomi to appoint new Sub-processors, and Nagomi shall comply with the conditions of this Section 5. The Sub-processor List as of the date of execution of this DPA is hereby authorized by the Customer. Customer shall send an email to privacy@nagomisecurity.com with the subject SUBSCRIPTION TO SUB-PROCESSORS NOTIFICATION, to subscribe to notifications of new Sub-processors, and if Customer subscribes, Nagomi shall provide notification of any new Sub-processor(s).

5.2 Customer may reasonably object to Nagomi's use of a Sub-processor for reasons related to the GDPR by notifying Nagomi promptly in writing within three (3) business days after receipt of Nagomi's notice in accordance with the mechanism set out in Section 1 and such written objection shall include the reasons related to the GDPR for objecting to Nagomi's use of such Sub-processor. Failure to object to such Sub-processor in writing within three (3) business days following Nagomi's notice shall be deemed as acceptance of the Sub-Processor. In the event Customer reasonably objects to a Sub-processor, as permitted in the preceding sentences, Nagomi will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's use of the Services to avoid Processing of Personal Data by the objected-to Sub-processor without unreasonably burdening the Customer. If Nagomi is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Nagomi without the use of the objected-to Sub-processor by providing written notice to Nagomi provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Nagomi. Customer will have no further claims against Nagomi due to the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA in the situation described in this paragraph.

5.3 This Section 5 shall not apply to subcontractors of Nagomi which provide ancillary services to support the performance of the DPA. This includes, for example, telecommunication services, maintenance and user service, cleaning staff, or auditors.

6. SECURITY

6.1 Taking into account the state of the art, the costs of implementation, the scope, the context, the purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Nagomi shall maintain all industry-standard technical and organizational measures required pursuant to Article 32 of the GDPR for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, as set forth in the Security Documentation which are hereby approved by Customer. Upon the Customer's request, Nagomi will use commercially reasonable efforts to assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing, the state of the art, and the information available to Nagomi.

6.2 Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement and this DPA, Nagomi shall make available to Customer that is not a competitor of Nagomi (or Customer's independent, third-party auditor that is not a competitor of Nagomi) a copy or a summary of Nagomi's then most recent third-party audits or certifications, as applicable (provided, however, that such audits, certifications and the results therefrom, including the documents reflecting the outcome of the audit and/or the certifications, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Nagomi's prior written approval and, upon Nagomi's first request, Customer shall return all records or documentation in Customer's possession or control provided by Nagomi in the context of the audit and/or the certification). At Customer's cost and expense, Nagomi shall allow for and contribute to audits, including inspections of Nagomi's, conducted by the controller or another auditor mandated by the controller (who is not a direct or indirect competitor of Nagomi) provided that the parties shall agree on the scope, methodology, timing and conditions of such audits and inspections. Notwithstanding anything to the contrary, such audits and/or inspections shall not contain any information, including without limitation, personal data that does not belong to Customer.

6.3 Nothing in this DPA will require Nagomi either to disclose to Customer (and/or its authorized auditors), or provide access to: (i) any data of any other customer of Nagomi; (ii) Nagomi's internal accounting or financial information; (iii) any trade secret of Nagomi; or (iv) any information that, in Nagomi's sole reasonable discretion, could compromise the security of any of Nagomi's systems or premises or cause Nagomi to breach obligations under any applicable law or its obligations to any third party.

7. **PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION.** Nagomi shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, including Personal Data, transmitted, stored or otherwise Processed by Nagomi of which Nagomi becomes aware (a "**Personal Data Incident**"). Nagomi shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Nagomi deems necessary, possible and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Nagomi reasonable control. In any event, Customer will be the party responsible for notifying supervisory authorities and/or concerned data subjects (where required by Data Protection Laws and Regulations).

8. **RETURN AND DELETION OF PERSONAL DATA.** Subject to the Agreement, Nagomi shall, at the choice of Customer, delete or return the Personal Data to Customer after the end of the provision of the Services relating to Processing, and shall delete existing copies unless applicable law requires storage of the Personal Data. In any event, to the extent required or allowed by applicable law, Nagomi may retain one copy of the Personal Data for evidence purposes and/or for the establishment, exercise or defence of legal claims and/or to comply with applicable laws and regulations. If the Customer requests the Personal Data to be returned, the Personal Data shall be returned in the format generally available for Nagomi's Customers.

9. **AUTHORIZED AFFILIATES**

9.1 The Parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Nagomi. Each Authorized Affiliate agrees to be bound by the obligations under this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Customer.

9.2 The Customer shall remain responsible for coordinating all communication with Nagomi under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10. **TRANSFERS OF DATA**

10.1 Personal Data may be transferred from the EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**"), the United Kingdom to countries that offer adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission, the UK supervisory authority ("**Adequacy Decisions**"), without any further safeguard being necessary.

10.2 To the extent that there is Processing of Personal Data which includes transfers from the EEA, the UK to countries which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision ("**Other Countries**"), the below terms shall apply:

a) With respect to the EU transfers of Personal Data, Customer as a Data Exporter (as defined in the SCCs) and Nagomi on behalf of itself and each Nagomi Affiliate (as applicable) as a Data Importer (as defined in the SCCs) hereby enter into the SCC set out in **Schedule 3**. To the extent that there is any conflict or inconsistency between the terms of the SCC and the terms of this DPA, the terms of the SCC shall take precedence.

b) With respect to the UK transfers of Personal Data (from the UK to other countries which have not been subject to a relevant Adequacy Decision), Customer as a Data Exporter (as defined in the UK SCCs) and Nagomi on behalf of itself and each Nagomi Affiliate (as applicable) as a Data Importer (as defined in the UK SCCs), hereby enter into the UK SCC set out in **Schedule 3**. To the extent that there is any conflict or inconsistency between the terms of the UK SCC and the terms of this DPA, the terms of the UK SCC shall take precedence.

11. **TERMINATION.** This DPA shall automatically terminate upon the termination or expiration of the Agreement under which the Services are provided. Sections 2.2, 2.3.3, 8 and 13 shall survive the termination or expiration of this DPA for any reason. This DPA cannot, in principle, be terminated separately to the Agreement, except where the Processing ends before the termination of the Agreement, in which case, this DPA shall automatically terminate.

12. **CCPA.** To the extent that the Personal Data is subject to the CCPA, Nagomi shall not sell or share Customer's Personal Data. Nagomi acknowledges that when processing Personal Data in the context of the provision of the Services, Customer is not selling or sharing Personal Data to Nagomi. Nagomi agrees not to retain, use or disclose Customer Personal Data: (i) for any purpose other than the Business Purpose (as defined below); (ii) for no other commercial or Business Purpose; or (iii) outside the direct business relationship between Nagomi and Customer. Notwithstanding the foregoing, Nagomi may use, disclose, or retain Customer Personal Data to: (i) transfer the Personal Data to other Nagomi's entities (including, without limitation, affiliates and subsidiaries), service providers, third parties and vendors, in order to provide the Services to Customer; (ii) to comply with, or as allowed by, applicable laws; (iii) to defend legal claims or comply with a law enforcement investigation; (ii) for internal use by Nagomi to build or improve the quality of its services and/or for any other purpose permitted under the CCPA; (iii) to detect data security incidents, or protect against fraudulent or illegal activity; and (iv) collect and analyse anonymous information. Nagomi shall use commercially reasonable efforts to comply with its obligations under CCPA. If Nagomi becomes aware of any material applicable requirement (to Nagomi as a service provider) under CCPA that Nagomi cannot comply with, Nagomi shall use commercially reasonable efforts to notify Customer. Upon written Customer's notice, Nagomi shall use commercial reasonable and appropriate steps to stop and remediate Nagomi's alleged unauthorized use of Personal Data; provided that Customer must explain and demonstrate in the written notice which processing activity of Personal Data it considers to be unauthorized and the applicable reasons. Nagomi shall use commercially reasonable efforts to enable Customer to comply with consumer requests made pursuant CCPA. Notwithstanding anything to the contrary, Customer shall be fully and solely responsible for complying with its own requirements under CCPA. "**Business purpose**" means the Processing activities that Nagomi will perform to provide Services (as described in the Agreement), this DPA and any other instruction from Customer, as otherwise permitted by applicable law, including, CCPA and the applicable regulations, or as otherwise necessary to provide the Services to Customer.

13. **RELATIONSHIP WITH AGREEMENT.** In the event of any conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement. Notwithstanding anything to the contrary in the Agreement and/or in any agreement between the parties and to the maximum extent permitted by law: (A) Nagomi's (including Nagomi's Affiliates') entire, total and aggregate liability, related to personal data or information, privacy, or for breach of, this DPA and/or Data Protection Laws and Regulations, including, without limitation, if any, any indemnification obligation or applicable law regarding data protection or privacy, shall be limited to the amounts paid to Nagomi under the Agreement within twelve (12) months preceding the event that gave rise to the claim. This limitation of liability is cumulative and not per incident; (B) In no event will Nagomi and/or Nagomi Affiliates and/or their third-party providers, be liable under, or otherwise in connection with this DPA for: (i) any indirect, exemplary, special, consequential, incidental or punitive damages; (ii) any loss of profits, business, or anticipated savings; (iii) any loss of, or damage to data, reputation, revenue or goodwill; and/or (iv) the cost of procuring any substitute goods or services; and (C) The foregoing exclusions and limitations on liability set forth in this Section shall apply: (i) even if Nagomi, Nagomi Affiliates or third-party providers, have been advised, or should have been aware, of the possibility of losses or damages; (ii) even if any remedy in this DPA fails of its essential purpose; and (iii) regardless of the form, theory or basis of liability (such as, but not limited to, breach of contract or tort).

14. **AMENDMENTS.** This DPA may be amended at any time by a written instrument duly signed by each of the Parties.

15. **LEGAL EFFECT.** Nagomi may assign this DPA or its rights or obligations hereunder to any Affiliate thereof, or to a successor or any Affiliate thereof, in connection with a merger, consolidation or acquisition of all or substantially all of its shares, assets or business relating to this DPA or the Agreement. Any Nagomi obligation hereunder may be performed (in whole or in part), and any Nagomi right (including invoice and payment rights) or remedy may be exercised (in whole or in part), by an Affiliate of Nagomi.

List of Schedules

- **SCHEDULE 1 - DETAILS OF THE PROCESSING**
- **SCHEDULE 2 - SUB-PROCESSOR LIST**
- **SCHEDULE 3 – STANDARD CONTRACTUAL CLAUSES**
- **SCHEDULE 4 – SECURITY DOCUMENTATION**

SCHEDULE 1 - DETAILS OF THE PROCESSING

Subject matter. Nagomi will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further instructed by Customer in its use of the Services.

Nature and Purpose of Processing.

1. Performing the Agreement, this DPA and/or other contracts executed by the Parties, including, providing the Service(s) to Customer and providing support and technical maintenance, if agreed in the Agreement.
2. To follow Customers' instructions.
3. For Nagomi to comply with documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement.

Duration of Processing. Subject to any Section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Nagomi will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data.

- Metadata, to the extent that it contains Personal Data (only when Customers instruct Nagomi to collect and store it)
- User details and privileges of the Customer's environments, which could include without limitation, identification and contact data (name, address, title, contact details, username), employment details (employer, job title, geographic location, area of responsibility); IT related data (computer ID, user ID, IP address, log files).
- Access logs and event details of the Customer's environments
- Any other Personal Data or information that the Customer decides to provide to Nagomi in connection with the Services.

For the avoidance of doubt, the information subject to the Nagomi's privacy policy (e.g., log-in details) available here: https://www.nagomisecurity.com/privacy-policy shall not be subject to the terms of this DPA.

Categories of Data Subjects.

- Customer's users authorized by Customer to use the Services
- Employees, agents, advisors, freelancers of Customer (who are natural persons)

The frequency of the transfer. Continuous basis

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period. As described in this DPA and/or the Agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing. As detailed in Schedule 2.

SCHEDULE 2 – SUB-PROCESSOR LIST

Entity Name	**Sub-Processing Activities**	**Hosting Country**
Amazon Web Services	Cloud-based storage of data.	United States and Germany
Nagomi Security Ltd., and Nagomi Security, Inc.	Provision of the Services and support	Israel and US (as applicable)

SCHEDULE 3 - STANDARD CONTRACTUAL CLAUSES

EU SCCs. If the Processing of Personal Data includes transfers from the EU to countries outside the EEA which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision, the Parties shall comply with Chapter V of the GDPR. The Parties hereby agree to execute the Standard Contractual Clauses as follows:

a) The Standard Contractual Clauses (Controller-to-Processor and Processor to Processor) as applicable, will apply, with respect to restricted transfers between Customer and Nagomi that are subject to the GDPR.

b) The Parties agree that for the purpose of transfer of Personal Data between Customer (as Data Exporter) and Nagomi (as Data Importer), the following shall apply: (i) Clause 7 of the Standard Contractual Clauses shall be not applicable; (ii) In Clause 9, option 2 shall apply and the method described in Section 5 of the DPA (Authorization Regarding Sub-Processors) shall apply; (iii) Clause 11 of the Standard Contractual Clauses shall be not applicable; (iv) In Clause 13: the relevant option applicable to the Customer, as informed by Customer to Nagomi; (v) In Clause 17, option 1 shall apply. The Parties agree that the Standard Contractual Clauses shall be governed by the laws of Ireland; and (vi) In Clause 18(b) the Parties choose the courts of Ireland, as their choice of forum and jurisdiction.

c) Annex I.A: With respect to Module Two: (i) Data Exporter is Customer as a data controller and (ii) the Data Importer is Nagomi as a data processor. With respect to Module Three: (i) Data Exporter is Customer as a data processor and (ii) the Data Importer is Nagomi as a data processor (sub-processor). Data Exporter and Data Importer Contact details: As detailed in the Agreement. Signature and Date: By entering into the Agreement and this DPA, each Party is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the DPA.

d) Annex I.B of the Standard Contractual Clauses shall be completed as described in Schedule 1 (Details of the Processing) of this DPA.

e) Annex I.C of the Standard Contractual Clauses shall be completed as follows: The competent supervisory authority is the Irish supervisory authority.

f) Annex II of the Standard Contractual Clauses shall be completed as described in the Security Documentation (Schedule 4).

g) Annex III of the Standard Contractual Clauses shall be completed with the authorized sub-processors detailed in Schedule 2 (Sub-processor list) of this DPA.

UK SCCs. If the Processing of Personal Data includes transfers from the UK to countries which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision, the Parties shall comply with Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018. The Parties hereby agree to execute the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as follows:

a) The UK Standard Contractual Clauses (Controller-to-Processor and Processor to Processor) if applicable, will apply with respect to restricted transfers between Customer and Nagomi that are subject to the GDPR.

b) The Parties agree that for the purpose of transfer of Personal Data between Customer (as Data Exporter) and Nagomi (as Data Importer), the following shall apply: (i) Clause 7 of the Standard Contractual Clauses shall be not applicable; (ii) In Clause 9, option 2 shall apply and the method described in Section 5 of the DPA (Authorization Regarding Sub-Processors) shall apply; (iii) Clause 11 of the Standard Contractual Clauses shall be not applicable; (iv) In Clause 17, option 1 shall apply. The Parties agree that the Standard Contractual Clauses shall be governed by the laws of England and Wales; and (v) In Clause 18(b) the Parties choose 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, as their choice of forum and jurisdiction. Which Parties may end this Addendum as set out in Section 19: Importer and/or Exporter, in accordance with the agreed terms of the DPA.

c) Annex I.A: With respect to Module Two: Data Exporter is Customer as a data controller and the Data Importer is Nagomi as a data processor. With respect to Module Three: Data Exporter is Customer as a data processor and the Data Importer is Nagomi as a data processor (sub-processor). Data Exporter and Data Importer Contact details: As detailed in the Agreement. Signature and Date: By entering into the Agreement and this DPA, each Party is deemed to have signed these UK Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the DPA.

d) Annex I.B of the UK Standard Contractual Clauses shall be completed as described in EU SCCS.

e) Annex I.C of the UK Standard Contractual Clauses: The competent supervisory authority is the ICO supervisory authority.

f) Annex II of the UK Standard Contractual Clauses shall be completed as described in EU SCCS.

g) Annex III of the UK Standard Contractual Clauses shall be completed as described in EU SCCS.

SCHEDULE 4 – SECURITY DOCUMENTATION

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

Security Control Category	**Description**
1. Governance	a. Assign to an individual or a group of individuals appropriate roles for developing, coordinating, implementing, and managing Vendor's administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Personal Data b. Use of data security personnel that are sufficiently trained, qualified, and experienced to be able to fulfill their information security-related functions
2. Risk Assessment	a. Conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls b. Maintain risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur c. Document formal risk assessments d. Review formal risk assessments by appropriate managerial personnel
3. Information Security Policies	a. Create information security policies, approved by management, published and communicated to all employees and relevant external parties. b. Review policies at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
4. Human Resources Security	a. Maintain policies requiring reasonable background checks of any new employees who will have access to Personal Data or relevant Vendor Systems, subject to local law b. Regularly and periodically train personnel on information security controls and policies that are relevant to their business responsibilities and based on their roles within the organization
5. Asset Management	a. Maintain policies establishing data classification based on data criticality and sensitivity b. Maintain policies establishing data retention and secure destruction requirements c. Implement procedures to clearly identify assets and assign ownership

6. Access Controls	a. Identify personnel or classes of personnel whose business functions and responsibilities require access to Personal Data, relevant Vendor Systems and the organization’s premises b. Maintain controls designed to limit access to Personal Data, relevant Vendor Systems and the facilities hosting the Vendor Systems to authorized personnel c. Review personnel access rights on a regular and periodic basis d. Maintain physical access controls to facilities containing Vendor Systems, including by using access cards or fobs issued to Vendor personnel as appropriate e. Maintain policies requiring termination of physical and electronic access to Personal Data and Vendor Systems after termination of an employee f. Implement access controls designed to authenticate users and limit access to Vendor Systems g. Implement policies restricting access to the data center facilities hosting Vendor Systems to approved data center personnel and limited and approved Vendor personnel h. Maintain dual layer access authentication processes for Vendor employees with administrative access rights to Vendor Systems
7. Cryptography	a. Implement encryption key management procedures b. Encrypt sensitive data using a minimum of AES/128 bit ciphers in transit and at rest
8. Physical Security	a. Require two factor controls to access office premises b. Register and escort visitors on premises
9. Operations Security	a. Perform periodic network and application vulnerability testing using dedicated qualified internal resources b. Contract with qualified independent 3rd parties to perform periodic network and application penetration testing c. Implement procedures to document and remediate vulnerabilities discovered during vulnerability and penetration tests
10. Communications Security	a. Maintain a secure boundary (e.g. using firewalls and network traffic filtering) b. Require internal segmentation to isolate critical systems from general purpose networks c. Require periodic reviews and testing of network controls
11. System Acquisition, Development and Maintenance	a. Assign responsibility for system security, system changes and maintenance b. Test, evaluate and authorize major system components prior to implementation
12. Supplier Relationships	Periodically review available security assessment reports of vendors hosting the Vendor Systems to assess their security controls and analyze any exceptions set forth in such reports