ORCA SECURITY SAAS LICENSE AGREEMENT

This Agreement (the "Agreement") is entered into on ____, __ 2021 (the "Effective Date"), by and between Orca Security Inc., a company incorporated under the laws of the State of Delaware having its principal place of business at 6630 Moore Drive Los Angeles, California, together with its affiliates (the "Company", "we", "us" or "our") and you, on behalf of yourself or your organization (the "Customer" or "you") (each, a "Party" and collectively, the "Parties"). You may use our software known as "Orca Cloud Visibility Platform" subject to the terms below:

1. **License.** Subject to the terms and conditions of this Agreement, Company hereby grants Customer a limited, non-exclusive, non-sublicensable, non-transferable and revocable license to remotely access (i.e. on a SaaS basis) the software ("**Platform**") and use it as well as any documentation (**"Documentation**") provided to you in connection with the Platform operation for internal purposes. You may only use the Platform in accordance with the Documentation, subject to the use limitations indicated in your proposal or order attached hereto as Exhibit A (**"Proposal**") and applicable laws.

2. **Services.** In addition to the abovementioned licenses, we may provide services, as detailed in the Proposal (collectively with the Platform, the "Services**"**). Support and maintenance services are provided according to our Service Level Agreement attached hereto as Exhibit B ("**SLA"**).

3. **Payment.** The Services are conditioned on Customer's upfront payment in full of the applicable fees set forth in the Proposal. Unless otherwise specified in the Proposal: (i) Customer will pay all amounts due under this Agreement in U.S. Dollars currency; and (ii) all amounts invoiced hereunder are due and payable within thirty (30) days of the date of the invoice. All amounts payable under this Agreement are exclusive of all sales, use, value-added, withholding, and other direct or indirect taxes, charges, levies and duties.

4. **Customer Account**. The Platform may only be used through a Customer account (the "**Account**"). Such Account may be accessed solely by Customer's employees or service providers who are explicitly authorized by Customer to use the Platform (each, a "**Permitted User**"). Customer will ensure that the Permitted Users keep the Account login details secure at all times and comply with the terms of this Agreement; and will be fully responsible for any breach of this Agreement by a Permitted User. Unauthorized access or use of the Account or the Platform must be immediately reported to the Company.

5. **Prohibited Uses.** Except as specifically permitted herein, without the prior written consent of the Company, Customer must not, and shall not allow any Permitted User or any third party to, directly or indirectly: (i) copy, modify, create derivative works of or distribute any part of the Platform (including by incorporation into its products); (ii) sell, license (or sub-license), lease, assign, transfer, pledge, or share Customer's rights under this Agreement with any third party; (iii) use any "open source" or "copyleft software" in a manner that would require the Company to disclose the source code of the Platform to any third party; (iv) disassemble, decompile, reverse engineer or attempt to discover the Platform's source code or underlying algorithms; (v) use the Platform in a manner that violates or infringes any rights of any third party, including but not limited to, privacy rights, publicity rights or intellectual property rights; (vi) remove or alter any trademarks or other proprietary notices related to the Platform; (vii) circumvent, disable or otherwise interfere with security-related features of the Platform or features that enforce use limitations; (viii) export, make available or use the Platform in any manner prohibited by applicable laws (including without limitation export control laws); and/or (ix) transmit any malicious code (*i.e.*, software viruses, Trojan horses, worms, malware or other computer instructions, devices, or techniques that erase data or programing, infect, disrupt, damage, disable, or shut down a computer system or any component of such computer system) or other unlawful material in connection with our Product. In addition, You may only disclose the results of any testing or benchmarking of the Platform if You also do not restrict and permit Customer's users/customers to disclose the results of any testing or benchmarking of Customer's products. If You do not allow such disclosure and benchmarking, You are restricted from disclosing the results of any testing or benchmarking of the Platform.

6. **Customer Data**. As we operate the Services, we may monitor data flows and logs transmitted between your wireless networks (the "**Customer Data**"). You shall be deemed the exclusive owner of the Customer Data.

7. **Warranties**. Each Party represents and warrants that it is duly organized, validly existing and in good standing under the laws of its jurisdiction of incorporation or organization; and that the execution and performance of this Agreement will not conflict with other agreements to which it is bound or violate applicable law and each Party shall comply with all applicable privacy laws.

8. **Intellectual Property Rights.** The Platform is not for sale and is the Company's sole property. All right, title, and interest, including any intellectual property rights evidenced by or embodied in, attached, connected, and/or related to the Platform and any and all improvements and derivative works thereof are and shall remain owned solely by Company or its licensors. This Agreement does not convey to Customer any interest in or to the Platform other than a limited right to use the Platform in accordance with Section 1. Nothing herein constitutes a waiver of the Company's intellectual property rights under any law.

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

9. **Third Party Components**. The Platform may use or include third party software, files, libraries or components that are subject to third party open source license terms ("**Open Source Licenses**"). The respective licenses or notices of such Open Source Licenses are available at https://orca.security/open_source_licenses and may be updated from time to time.

10. **Confidentiality**. Each Party may have access to certain non-public and/or proprietary information of the other Party, in any form or media, including without limitation trade secrets and other information related to the products, software, technology, data, know-how, or business of the other Party, and any other information that a reasonable person should have reason to believe is proprietary, confidential, or competitively sensitive (the "**Confidential Information**"). The Documentation shall be considered as Confidential Information hereunder. Each Party shall take reasonable measures, at least as protective as those taken to protect its own confidential information, but in no event less than reasonable care, to protect the other Party's Confidential Information from disclosure to a third party. The receiving party's obligations under this Section, with respect to any Confidential Information of

the disclosing party, shall not apply to and/or shall terminate if such information: (a) was already lawfully known to the receiving party at the time of disclosure by the disclosing party; (b) was disclosed to the receiving party by a third party who had the right to make such disclosure without any confidentiality restrictions; (c) is, or through no fault of the receiving party has become, generally available to the public; (d) was independently developed by the receiving party without access to, or use of, the disclosing party's Confidential Information; or (e) is required to be disclosed to satisfy any applicable law, regulation, legal process, subpoena or governmental request. Neither Party shall use or disclose the Confidential Information of the other Party except for performance of its obligations under this Agreement ("**Permitted Use**"). The receiving party shall only permit access to the disclosing party's Confidential Information to its respective employees, consultants, affiliates, agents and subcontractors having a need to know such information in connection with the Permitted Use, who either (i) have signed a non-disclosure agreement with the receiving party containing terms at least as restrictive as those contained herein or (ii) are otherwise bound by a duty of confidentiality to the receiving party at least as restrictive as the terms set forth herein. The receiving party will be allowed to disclose Confidential Information to the extent that such disclosure is required by law or by the order or a court of similar judicial or administrative body, provided that it notifies the disclosing Party of such required disclosure to enable disclosing party to seek a protective order or otherwise prevent or restrict such disclosure. All right, title and interest in and to Confidential Information are and shall remain the sole and exclusive property of the disclosing Party.

11. **LIMITED WARRANTIES.** The Company represents and warrants that, under normal authorized use, the Platform shall substantially perform in conformance with its Documentation. As the Customer's sole and exclusive remedy and the Company's sole liability for breach of this warranty, the Company shall use commercially reasonable efforts repair the Platform in accordance with the SLA. The warranty set forth shall not apply if the failure of the Platform results from or is otherwise attributable to: (i) repair, maintenance or modification of the Platform by persons other than the Company or its authorized contractors; (ii) accident, negligence, abuse or misuse of the Platform by Customer; (iii) use of the Platform by Customer other than in accordance with the Documentation; (iv) Customer's failure to implement software updates provided by the Company specifically to avoid such failure; or (v) the combination of the Platform with equipment or software not authorized or provided by the Company. OTHER THAN AS EXPLICITLY STATED IN THIS AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE PLATFORM, ANY REPORTS OR OTHER OUTPUT (THE **"REPORTS"**) AND SERVICES ARE PROVIDED ON AN "AS IS" BASIS. THE COMPANY DOES NOT WARRANT THAT THE PLATFORM, THE REPORTS AND/OR THE SERVICES WILL MEET CUSTOMER'S REQUIREMENTS. EXCEPT AS SET FORTH IN SECTION 7 AND THIS SECTION 11, THE COMPANY EXPRESSLY DISCLAIMS ALL EXPRESS WARRANTIES AND ALL IMPLIED WARRANTIES, INCLUDING MERCHANTABILITY, TITLE, NON-INTERFERENCE, FITNESS FOR A PARTICULAR PURPOSE.

12. **LIMITATION OF LIABILITY**. EXCEPT FOR THE COMPANY INDEMNIFICATON OBLIGATION UNDER SECTION 13, ANY DAMAGES RESULTING FROM ANY BREACH OF EITHER PARTY'S CONFIDENTIALITY OBLIGATIONS HEREIN; EITHER PARTY'S WILLFUL MISCONDUCT, FRAUD OR VIOLATION OF LAW AND/OR CUSTOMER'S (C) MISAPPROPRIATION OR OTHERWISE VIOLATION OF COMPANY'S INTELLECTUAL PROPERTY RIGHTS (INCLUDING MISUSE OF THE LICENSE BY CUSTOMER PURSUANT TO SECTION 1); NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF REVENUE, REPUTATION, OR PROFITS, DATA, OR DATA USE.

EXCEPT FOR THE COMPANY INDEMNIFICATION OBLIGATION UNDER SECTION 13, ANY DAMAGES RESULTING FROM ANY BREACH OF EITHER PARTY'S CONFIDENTIALITY OBLIGATIONS HEREIN; A PARTY'S WILLFUL MISCONDUCT, FRAUD OR VIOLATION OF LAW, AND/OR DAMAGES RESULTING FROM CUSTOMER'S MISAPPROPRIATION OR OTHERWISE VIOLATION OF COMPANY'S INTELLECTUAL PROPERTY RIGHTS (INCLUDING MISUSE OF THE LICENSE BY CUSTOMER PURSUANT TO SECTION 1); EITHER PARTY'S MAXIMUM LIABILITY FOR ANY DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT OR TORT, OR OTHERWISE, SHALL IN NO EVENT EXCEED, IN THE AGGREGATE, THE TOTAL AMOUNTS ACTUALLY PAID TO COMPANY IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM. THIS LIMITATION OF LIABILITY IS CUMULATIVE AND NOT PER INCIDENT. FOR CLARITY, THE LIMITATIONS IN THIS SECTION DO NOT APPLY TO PAYMENTS DUE TO COMPANY UNDER THIS AGREEMENT (INCLUDING THE PROPOSAL).

13. **Indemnification**. Company acknowledges and agrees to defend, at its expense, any third party action or suit brought against the Customer alleging that the Platform, when used as permitted under this Agreement, infringes intellectual property rights of a third party (**"IP Infringement Claim"**); and the Company will pay any damages awarded in a final judgment against the Customer that are attributable to any such claim, provided that (i) the Customer promptly notifies the Company in writing of such claim; and (ii) the Customer grants the Company the sole authority to handle the defense or settlement of any such claim and provides the Company with all reasonable information and assistance, at Company's expense. The Company will not be bound by any settlement that the Customer enters into without the Company's prior written consent.

If the Platform becomes, or in the Company's opinion is likely to become, the subject of an IP Infringement Claim, then the Company may, at its sole discretion: (a) procure for the Customer the right to continue using the Platform; (b) replace or modify the Platform to avoid the IP Infringement Claim; or (c) if options (a) and (b) cannot be accomplished despite the Company's reasonable efforts, then the Company may terminate this Agreement and in such event accept return of the affected Platform and provide a refund for any amount pre-paid by Customer for such returned Platform for the remaining unused period of the license.

Notwithstanding the foregoing, the Company shall have no responsibility for IP Infringement Claims resulting from or based on: (i) modifications to the Platform made by a party other than the Company or its designee; (ii) the Customer's failure to implement software updates provided by the Company specifically to avoid infringement; or (iii)

combination or use of the Platform with equipment, devices or software not supplied by the Company or not in accordance with the Documentation.

This Section states Company's entire liability, and Customer's exclusive remedy, for claims or alleged or actual infringement.

14. **Privacy.** To the extent that Customer needs a data processing agreement, Customer and Company shall enter into the Data Processing Agreement attached as **Exhibit C ("DPA")**.

15. **Term and Termination.** This Agreement shall enter into force and effect on the Effective Date and shall remain in full force and effect for the period specified in the Proposal ("**Initial Term**") and shall be renewed for successive one (1) year terms upon both parties written consent (each a "**Renewal Term**" and together with the Initial Term, the "**Term"**), unless terminated earlier as set forth herein and/or either Party provides at least 30 days prior written notice of non-renewal. Either Party may terminate this Agreement with immediate effect if the other Party materially breaches this Agreement and such breach remains uncured fifteen (15) days after having received written notice thereof. Upon termination or expiration of this Agreement: (i) Platform license granted to Customer under this Agreement shall expire, and Customer shall discontinue any further use and access thereof; (ii) Customer shall immediately delete and dispose of all copies of the Documentation in Customer's or any of its representatives' possession or control; (iii) Company shall return and/or permanently delete (as instructed by Customer) all Customer Data**;** and (iv) Customer shall not be relieved of its duty to discharge in full all due sums owed by Customer to Company under this Agreement until the date of termination or expiration hereof. The provisions of this Agreement that, by their nature and content, must survive the termination of this Agreement in order to achieve the fundamental purposes of this Agreement shall so survive. If applicable, Customer shall be responsible to download its Customer Data prior to termination of this Agreement. The termination of this Agreement shall not limit either Party from pursuing any other remedies available to it under applicable law.

16. **Miscellaneous.** This Agreement - including any Proposals, and any exhibits attached or referred hereto - represents the complete agreement concerning the subject matter hereof and may be amended only by a written agreement executed by both Parties. The failure of either Party to enforce any rights granted hereunder or to take action against the other Party in the event of any breach hereunder shall not be deemed a waiver by that Party as to subsequent enforcement of rights or subsequent actions in the event of future breaches. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any use of the Platform by an agency, department, or other entity of the United States government shall be governed solely by the terms of this Agreement. Neither Party may assign its rights or obligations under this Agreement without the prior written consent of the other Party, which consent may not be unreasonably withheld or delayed. Company may, in its reasonable discretion, use Customer's name and logo on its website and in its marketing materials as a reference customer. Media releases and public announcements or disclosures relating to this Agreement, its subject matter or the potential business transaction between the Parties shall be coordinated with and consented to by both Parties in writing prior to the release thereof. This Agreement shall be governed by and construed under the laws of the State of New York, without reference to principles and laws relating to the conflict of laws. The competent courts of New York shall have the exclusive jurisdiction with respect to any dispute and action arising under or in relation to this Agreement. This Agreement does not, and shall not be construed to create any relationship, partnership, joint venture, employer-employee, agency, or franchisor-franchisee relationship between the Parties. Either Party will not be liable for any delay or failure to perform its obligations resulting from circumstances or causes beyond the reasonable control of the Company. This Agreement may be executed in electronic counterparts, each of which counterpart, when so executed and delivered, shall be deemed to be an original and all of which counterparts, taken together, shall constitute but one and the same agreement.

* * * * * * * *

IN WITNESS HEREOF, the Parties have caused this Agreement to be executed by their duly authorized representatives to be effective as of the Effective Date.

Orca Security Inc.

Name: _____

Title: _____

Date: _____

Name: _____

Title: _____

Date: _____

Exhibit A

The Proposal

Exhibit B

SERVICE LEVEL AGREEMENT (SLA)

Company reserves the right to change the terms of this SLA by providing Customer with at least thirty (30) days prior written notice.

During the term of the Agreement, Company will use commercially reasonable efforts to make the Service available with a Monthly Uptime Percentage (defined below) of at least 99.9% during monthly billing cycle (the "**Service Commitment**"). In the event that Company does not meet the Service Commitment, the Customer will be eligible to receive a Service Credit (defined below) as described below.

The following definitions apply to this SLA:

- "**Company Service(s)**" or "**Service(s)**" means the services specified in the Agreement;
- "**Downtime**" or "**Downtime Incident**" means the time in which Company Service is unavailable to the Customer as measured and determined solely by Company based on its servers. Downtime Incidents shall exclude: planned downtime incidents announced in-advance by Company, including without limitation, for periodic upgrade and maintenance; and/or any time where Company is awaiting information from the Customer or awaiting Customer confirmation that the Service has been restored.
- "**Downtime Period**" means the number of minutes in a calendar month during which Company Service is unavailable to the Customer due to Downtime Incident(s).
- "**Monthly Uptime Percentage**" means the total number of minutes in a calendar month, minus the Downtime Period, divided by the total number of minutes in a calendar month.
- "**Service Credit**" means credit notes due to the Customer as a result of Downtime Period as detailed in the following table:

Monthly Uptime Percentage	Percentage of monthly service license for Service which does not meet SLA that will be credited to future billing cycle for the Customer (in accordance with the subscription period applicable to each Customer)
Between 99.0% – 99.9% (inclusive)	10%
Less than 99.0%	20%

Service Credit Eligibility

If the Monthly Uptime Percentage is less than or equals 99.9%, then the Customer will be eligible to receive Service Credits as detailed in the table above.

In order to receive any of the Service Credits described above, the Customer must (i) notify Company's technical support team within thirty (30) days from the time on which the Customer becomes eligible to receive Service Credits; and (ii) submit Company's technical support team all information necessary for Company to validate the Customer's claim, including but not limited to: (a) a detailed description of the Downtime Incident; (b) information regarding the time and duration of the Downtime Incident. Failure to comply with these requirements will forfeit such Customer's right to receive Service Credits. In addition, the Customer must be in compliance with the Agreement in order to be eligible for a Service Credit.

Maximum Service Credits

The aggregate maximum number of Service Credits to be issued by Company to the Customer for any and all Downtime Periods that occur in a single subscription period shall not exceed 20% of the amount due by Customer for the Company Services provided to it during the applicable subscription period.

The Service Credits will be made in the form of a monetary credit applied to future use of the Company Services and will be deducted from the Customer's next billing cycle/invoice. The Service Credits will not entitle the Customer to any refund or other payment from Company.

THE CUSTOMER HEREBY ACKNOWLEDGES AND AGREES THAT ITS RIGHT TO RECEIVE SERVICE CREDITS AS SPECIFIED ABOVE CONSTITUTES ITS SOLE AND EXCLUSIVE REMEDY FOR ANY DOWNTIME INCIDENTS, UNAVAILABILITY OR NON-PERFORMANCE.

Other SLA Exclusions

The SLA does not apply to any: (a) features or services excluded from the Agreement (as specified in the associated Documentation); or (b) Downtime Incidents that: (i) are explicitly excluded under this SLA; (ii) are caused by factors beyond Company' reasonable control (e.g. any force majeure event, Internet access or related problems beyond Company' reasonable control etc.); (iii) results or outcomes attributable to repair, maintenance or modification of Company' software by persons other than Company' authorized third parties; (iv) resulted from accident, negligence, abnormal physical or electrical stress, abnormal environmental conditions, abuse or misuse of the Company' software; (v) resulted from use of the Company' software other than in accordance with its manuals, specifications or documentation or in violation of the Agreement; (vi) resulted from Customer's equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within Company' direct control); and/or (vii) resulted from the combination of the Company' software with equipment or software not authorized or provided by Company or otherwise approved by Company in the software's manuals, specifications or documentation.

Exhibit C (Only If Applicable. Orca Security DOES NOT require signing it, and if it isn't required from the customer perspective, it can be completely removed)

DATA PROCESSING AGREEMENT/ADDENDUM

This Data Processing Agreement ("**DPA**") is made and entered into as of this ____ day of ____, 2021 forms part of the SaaS License Agreement (the "**Agreement**"). You acknowledge that you, on behalf of [_____] incorporated under _____ law, with its principal offices located at _____ ("**Organization**") (collectively, **"You", "Your", "Client", or "Data Controller"**) have read and understood and agree to comply with this DPA, and are entering into a binding legal agreement with **Orca Security Inc.** as defined below (**"Orca"**, **"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) of GDPR-protected individuals. Both parties shall be referred to as the "Parties" and each, a "Party".

WHEREAS, Orca shall provide the services set forth in the Agreement (collectively, the "**Services**") for Client, 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.

1.2 References to clauses or sections are references to the clauses or sections of this DPA unless otherwise stated.

1.3 Words used in the singular include the plural and vice versa, as the context may require.

1.4 Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

1.5 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 Client'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 Client and Orca, but has not signed its own agreement with Orca and is not a "Client" 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 yourself, the Organization and/or the Organization's Authorized Affiliates.

(d) **"Data Protection Laws and Regulations"** means all laws and regulations, including, without limitation, laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

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

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

(g) "**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).

(h) **"Personal Data"** 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.

(i) **"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.

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

(k) **"Security Documentation"** means the Security Documentation applicable to the specific Services purchased by Client, as updated from time to time. By making a request to privacy@orca.security, Orca will send the Security Documentation.

(l) "**Orca**" means the relevant Orca entity of the following Orca legal entities: Orca Security Ltd and Orca Security Inc.

(m) "**Orca Group**" means Orca and its Affiliates engaged in the Processing of Personal Data.

(n) **"Sub-processor"** means any Processor engaged by Orca and/or Orca.

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

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data, (i) Client is the Data Controller, (ii) Orca is the Data Processor and that (iii) Orca or members of the Orca Group may engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2 **Client's Processing of Personal Data.** Client 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. For the avoidance of doubt, Client's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Client shall have sole responsibility for the means by which Client acquired Personal Data. Without limitation, Client 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 have any and all required legal bases in order to collect, Process and transfer to Orca the Personal Data and to authorize the Processing by Orca of the Personal Data which is authorized in this DPA. Client shall defend, hold harmless and indemnify Orca, its Affiliates and subsidiaries (including without limitation their directors, officers, agents, subcontractors and/or employees) from and against any liability of any kind related to any breach, violation or infringement by Client and/or its authorized users of any Data Protection Laws and Regulations and/or this DPA and/or this Section.

2.3 **Orca's Processing of Personal Data.**

2.3.1 Subject to the Agreement, Orca shall Process Personal Data in accordance with Client's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and this DPA and to provide the Services; (ii) Processing for Client to be able to use the Services; (iii) Processing to comply with other documented reasonable instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement; (iv) Processing as required by Union or Member State law to which Orca is subject; in such a case, Orca shall inform the Client of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.3.2 To the extent that Orca cannot comply with a request from Client and/or its authorized users relating to Processing of Personal Data (including, without limitation, any instruction, direction, code of conduct, certification, or change of any kind), Orca (i) shall inform Client, providing relevant details of the problem, (ii) Orca may, without any kind of liability towards Client, 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 Client shall pay to Orca all the amounts owed to Orca or due before the date of termination. Client will have no further claims against Orca (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).

2.3.3 Orca will not be liable in the event of any claim brought by a third party, including, without limitation, a Data Subject, arising from any act or omission of Orca, to the extent that such is a result of Client's instructions.

2.3.4 If Client provides Orca or any of the entities of the Orca Group with instructions, requests, suggestions, comments or feedback (whether orally or in writing) with respect to the Services, Client acknowledges that any and all rights, including intellectual property rights, therein shall belong exclusively to Orca and that such shall be considered Orca's intellectual property without restrictions or limitations of any kind, and Client hereby irrevocably and fully transfers and assigns to Orca any and all intellectual property rights therein and waives any and all moral rights that Client may have in respect thereto.

2.4 **Details of the Processing.** The subject-matter of Processing of Personal Data by Orca is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose 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.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Request.** Orca shall, to the extent legally permitted, promptly notify Client if Orca receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, erasure ("right to be forgotten"), restriction of Processing, data portability, right to object, or its right not to be subject to automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, Orca shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, Orca shall upon Client's request provide commercially reasonable efforts to assist Client in responding to such Data Subject Request, to the extent Orca is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Client shall be responsible for any costs arising from Orca's provision of such assistance.

4. ORCA PERSONNEL

4.1 **Confidentiality.** Orca shall ensure that its personnel engaged in the Processing of Personal Data have committed themselves to confidentiality and non-disclosure.

4.2 Orca 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, Orca shall inform the Client 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 its legal counsel(s), data protection advisor(s) and accountant(s).

5. AUTHORIZATION REGARDING SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Client acknowledges and agrees that (a) Orca's Affiliates may be used as Sub-processors; and (b) Orca and/or Orca's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.

5.2 **List of Current Sub-processors and Notification of New Sub-processors.**

5.2.1 Orca shall make available to Client the current list of Sub-processors used by Orca via privacy@orca.security. Such Sub-processor list shall include the identities and details of those Sub-processors and their country of location ("**Sub-processor List**"). The Sub-processor List as of the date of execution of this DPA, or as of the date of publication (as applicable), is hereby, or shall be (as applicable), authorized by Client. In any event, the Sub-processor List shall be deemed authorized by Client unless it provides a written reasonable objection for reasons related to the GDPR within ten (10) business days following the publication of the Sub-processor List. Client may reasonably object for reasons related to the GDPR to Orca's use of an existing Sub-processor by providing a written objection to privacy@orca.security. In the event Client reasonably objects to an existing Sub-processor, as permitted in the preceding sentences, and the parties do not find a solution in good faith to the issue in question, then Client may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Orca without the use of the objected-to Sub-processor by providing written notice to Orca provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Orca. Client will have no further claims against Orca due to (i) past use of approved Sub-processors prior

to the date of objection or (ii) the termination of the Agreement (including, without limitation, requesting refunds) and the DPA in the situation described in this paragraph.

5.2.2 Client may subscribe to notifications of new Sub-processors via privacy@orca.security, to which Client shall subscribe, and if Client subscribes, Orca shall provide notification of any new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the Services.

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

5.4 **Agreements with Sub-processors**. Orca shall respect the conditions referred to in Articles 28.2 and 28.4 of the GDPR when engaging another processor for Processing Personal Data provided by Client. In accordance with Articles 28.7 and 28.8 of the GDPR, if and when the European Commission lays down the standard contractual clauses referred to in such Article, the Parties may revise this DPA in good faith to adjust it to such standard contractual clauses.

6. SECURITY

6.1 **Controls for the Protection of Personal Data.** Orca 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 Client. Orca regularly monitors compliance with these measures. Upon the Client's request, Orca will assist Client, at Client'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 and the information available to Orca.

6.2 **Third-Party Certifications and Audits.** Upon Client's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement and this DPA, Orca shall make available to Client that is not a competitor of Orca (or Client's independent, third-party auditor that is not a competitor of Orca) a copy of Orca'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 Client to assess compliance with this DPA and/or with applicable Data Protection Laws and Regulations, and shall not be used for any other purpose or disclosed to any third party without Orca's prior written approval and, upon Orca's first request, Client shall return all records or documentation in Client's possession or control provided by Orca in the context of the audit and/or the certification). At Client's cost and expense, Orca shall allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (who is not a direct or indirect competitor of Orca) provided that the parties shall agree on the scope, timing and conditions of such audits and inspections.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

Orca maintains security incident management policies and procedures specified in Security Documentation and, to the extent required under applicable Data Protection Laws and Regulations, shall notify Client 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 Orca or its Sub-processors of which Orca becomes aware (a "**Personal Data Incident**"). Orca shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Orca deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Orca's reasonable control. The obligations herein shall not apply to incidents that are caused by Client or Client's users. In any event, Client 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, Orca shall, at the choice of Client, delete or return the Personal Data to Client 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, Orca may retain one copy of the Personal Data for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or to comply with applicable laws and regulations. If the Client requests the Personal Data to be returned, the Personal Data shall be returned in the format generally available for S Orca's Clients.

9. AUTHORIZED AFFILIATES

9.1 **Contractual Relationship.** The Parties acknowledge and agree that, by executing the DPA, the Client 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 Orca. 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 Client.

9.2 **Communication.** The Client shall remain responsible for coordinating all communication with Orca 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 **Transfers to countries that offer adequate level of data protection**: Personal Data may be transferred from the EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) and the United Kingdom (collectively, "**EEA**") 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 ("**Adequacy Decisions**"), without any further safeguard being necessary.

10.2 **Transfers to other countries**: If the Processing of Personal Data includes transfers from the EEA to countries which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision ("**Other Countries**"), the Parties shall comply with Article 46 of the GDPR, including, if necessary, executing the standard data protection clauses adopted by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission or comply with any of the other mechanisms provided for in the GDPR for transferring Personal Data to such Other Countries.

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, 2.3.4 and 12 shall survive the termination or expiration of this DPA for any reason.

12. **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: (A) Orca's (including Orca's Affiliates') entire, total and aggregate liability, related to, or for breach of, this DPA and/or Data Protection Laws and Regulations, including, if any, any indemnification obligation under the Agreement or applicable law regarding data protection or privacy, shall be limited to the amounts paid to Orca 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 Orca and/or Orca 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 Orca, Orca 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).

13. **AMENDMENTS**

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

14. LEGAL EFFECT

This DPA shall only become legally binding between Client and Orca when the formalities steps set out in the Section "INSTRUCTIONS ON HOW TO EXECUTE THIS DPA" below have been fully

completed.

15. SIGNATURE

The Parties represent and warrant that they each have the power to enter into, execute, perform and be bound by this DPA.

You, as the signing person on behalf of Client, represent and warrant that you have, or you were granted, full authority to bind the Organization and, as applicable, its Authorized Affiliates to this DPA. If you cannot, or do not have authority to, bind the Organization and/or its Authorized Affiliates, you shall not supply or provide Personal Data to Orca.

By signing this DPA, Client enters into this DPA on behalf of itself and, to the extent required or permitted under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent that Orca processes Personal Data for which such Authorized Affiliates qualify as the/a "data controller".

This DPA has been pre-signed on behalf of Orca.

Instructions on how to execute this DPA.

1. To complete this DPA, you must complete the missing information; and
2. Send the completed and signed DPA to us by email, indicating the Client's name, to privacy@orca.security

List of Schedules

- SCHEDULE 1 - DETAILS OF THE PROCESSING

The parties' authorized signatories have duly executed this Agreement:

CLIENT:

Signature:
Client Legal Name:
Print Name:
Title:
Date:

ORCA [*]

Signature:
Legal Name: Avi Shava
Print Name: Avi Shava
Title: CEO
Date:

SCHEDULE 1 - DETAILS OF THE PROCESSING

Subject matter

Orca will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further instructed by Client in its use of the Services.

Nature and Purpose of Processing

1. Providing the Service(s) to Client.
2. Scanning customer compute environment, including ones that include personal data, with the purpose to 1) detect security issues such as vulnerabilities, misconfiguration, compromises and other security issues and 2) provide the customer with detailed information about his environment.
3. Presenting customer with the outcome of scanning as written at section #2 above.
4. Setting up profile(s) for users authorized by Clients.
5. For Client to be able to use the Services.
6. For Orca to comply with documented reasonable instructions provided by Client where such instructions

are consistent with the terms of the Agreement.
7. Performing the Agreement, this DPA and/or other contracts executed by the Parties.
8. Providing support and technical maintenance, if agreed in the Agreement.
9. Resolving disputes.
10. Enforcing the Agreement, this DPA and/or defending Orca's rights.
11. Management of the Agreement, the DPA and/or other contracts executed by the Parties, including fees payment, account administration, accounting, tax, management, litigation; and
12. Complying with applicable laws and regulations, including for cooperating with local and foreign tax authorities, preventing fraud, money laundering and terrorist financing.
13. All tasks related with any of the above.

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, Orca will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data

Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- User names and login history data
- First name
- Last name
- Address
- Phone number
- Email address
- Payment information
- Any other Personal Data or information that the Client decides to provide to the Orca or the Services.
- Any other personal data or information involved in the detection of security issues in the customer environment.

The Client and the Data Subjects shall provide the Personal data to Orca by supplying the Personal data to Orca's Service.

In some limited circumstances Personal Data may also come from others sources, for example, in the case of anti-money laundering research, fraud detection or as required by applicable law. For clarity, Client shall always be deemed the "Data Controller" and Orca shall always be deemed the "Data Processor" (as such terms are defined in the GDPR).

Categories of Data Subjects

Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Client's customers and/or clients
- Client's users authorized by Client to use the Services
- Employees, agents, advisors, freelancers of Client (who are natural persons)
- Prospects, Clients, business partners and vendors of Client (who are natural persons)
- Employees or contact persons of Client's prospects, Clients, business partners and vendors
- Any personal data that exists on the scanned assets while scanning them for security incidents.