MASTER SERVICE TERMS

THESE MASTER SERVICE TERMS AND CONDITIONS (THESE "MASTER TERMS") APPLY TO THE PROVISION OF ACCESS TO THE SERVICES (DEFINED BELOW) AND RELATED SERVICES PURSUANT TO THE PROPOSAL OR ORDER FORM INTO WHICH THESE MASTER TERMS ARE INCORPORATED BY REFERENCE (THE "ORDER FORM") SIGNED OR OTHERWISE AGREED TO BY CUSTOMER. CAPITALIZED TERMS USED, BUT NOT DEFINED, HEREIN WILL HAVE THE MEANINGS SET FORTH IN THE ORDER FORM.

1. **DEFINITIONS**.

1.1 "Affiliate" means with respect to an entity, any entity that, directly or indirectly, controls, is owned or controlled by, or is under common control with, such entity. "Control," for purposes of this Section 1.1, means the ownership or control of more than fifty percent (50%) of all the voting power of the shares (or other securities or rights) entitled to vote for the election of directors or other governing authority.

1.2 "Agreement" means the Order Form and these Master Terms, and all attachments, exhibits, work orders, and schedules hereto, as well as any amendments hereto.

1.3 "Confidential Information" shall mean any information in any medium of a party (the "Disclosing Party") that is disclosed before or after the Effective Date to the other party (the "Receiving Party") in written or electronic form and marked "Confidential" or "Proprietary", or, if disclosed orally, which the Disclosing Party has indicated is confidential or proprietary, or any other information disclosed, which the Receiving Party, under the circumstances surrounding its disclosure, should reasonably know is treated as confidential and proprietary information of the Disclosing Party. Without limiting the foregoing, Confidential Information includes the terms of this Agreement, the Documentation, and any Intellectual Property, trade secrets, know-how, inventions, techniques, processes, algorithms, models, software programs (object or source code), financial information, product plans, employee lists, business manuals, special operating procedures, computer codes, policies and procedures, technologies or theories, sales and marketing plans and business information of a party.

1.4 "Customer Data" means all information and data entered by or on behalf of Customer or uploaded by Customer or on its behalf in connection with the Platform.

1.5 "Documentation" shall mean the technical documentation that is associated with the Services and that Simple Security makes available to Customer.

1.6 "Intellectual Property" shall mean all intellectual property rights, including copyrights, patents, trade secrets, trademarks/service marks and other proprietary rights.

1.7 "Law(s)" shall mean any and all laws, rules, regulations, codes or other obligations applicable to a party in its performance under this Agreement.

1.8 "Services" means the software-as-a-service solutions and any related Software provided under an Order Form.

1.9 "Party" means Customer or Simple Security Inc. (Simple Security), respectively.

1.10 "Personal Information" means any data or information from which a specific individual may be identified, contacted or located or that qualifies as "personal" or "private" information under any law applicable to the processing of such data or information pursuant to this Agreement.

1.11 "Platform" means Simple Security's subscription software as a service product and the databases, software, and other technology used by or on behalf of Simple Security to operate the Platform, including any third party technology

or services used by Simple Security to deliver operate the Platform, and the underlying data, content, information and software code thereof.

1.12 "Platform Integration" means any technical or operational integration, implemented or to be implemented by the parties pursuant to this Agreement of the Customer systems and the Platform that may enable Customer to utilize the Services.

1.13 "Users" shall mean employees, agents and independent contractors of Customers who are authorized by Customer to use the Platform.

2. **MASTER TERMS AND CONDITIONS**.

2.1 License.

(a) Scope of Services. Subject to the terms and conditions of this Agreement, Simple Security hereby grants to Customer a revocable, non-assignable, non-transferable, license and right, during the Term (as defined below): (a) to access and use the Services for Customer's internal business purposes; and (b) use, copy, reproduce, integrate, and distribute the Documentation, in whole or in part, solely as necessary in support of the use of Services by Customer. Nothing in this Agreement shall be construed as limiting in any manner the marketing or distribution activities of Simple Security or its licensors or Simple Security's appointment of other dealers, distributors, licensees or agents.

To the extent the Services enable Customer to download and install software applications owned or operated by Simple Security and used to facilitate access and use of the Platform and to perform system monitoring, in object code format only (the "Software") on Customer systems, then subject to the terms and conditions of this Agreement, Simple Security hereby grants Customer a nonexclusive, nontransferable, non-sublicensable right and license to download and install such Software on such systems and to use the Software to access and use the Platform as permitted by this Agreement. The Software may contain or be provided together with open source software ("Open Source Software"). Each item of Open Source Software is licensed under the terms of the license that accompanies such Open Source Software. Nothing in this Agreement limits grants rights that supersede, the terms and conditions of any applicable license for the Open Source Software.

(b) Integration. Customer will be responsible for its own costs incurred in connection with implementing the Platform Integration. Customer shall provide to Simple Security all information and materials that are necessary or reasonably requested by Simple Security to enable Simple Security to properly configure the Services via the Platform Integration and to operate the Services.

(c) Integration Maintenance and Support. Each Party shall provide and maintain the Party's own systems relevant to the Platform Integration during the Term and maintain all such systems in accordance with generally accepted industry standards. A Party will promptly notify the other Party in the event that it reasonably believes that: (a) maintenance or modifications to be performed on its systems may materially impair the other Party's ability to perform its obligations under this Agreement; or (b) technical, operational, or other issues affecting its systems or business may materially impair the availability or performance of the Platform Integration.

(d) Restrictions. Customer agrees not to, nor allow its Users or other third parties to, use the Services for any purposes beyond the scope of the license granted in this Agreement. Except as otherwise expressly set forth in this Agreement, Customer shall not (nor shall it permit or assist any third party) at any time, directly or indirectly: (i) copy, modify, or create derivative works of the Services , in whole or in part; (ii) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, or otherwise make available the Services ; (C) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to the source code of the Services, in whole or in part; (iii) alter or impair the functionality of the Services, disable, interfere with, or disrupt the performance of any aspect of the Services (including without limitation any security or license protection feature) or third-party data contained therein, (iv) input any data not intended for storage

or use on the Platform including, without limitation, social security numbers, location of persons, health information, driver's license, or passport or visa number ("Prohibited Data") or derive such Prohibited Data from the Services, (v) use the Services to create a competing service or software during or after the term of the Agreement, (vi) use the Services in a manner that is contrary to applicable law or in violation of any third party rights of privacy or intellectual property rights, (vii) remove or alter any proprietary notices brand labels or Intellectual Property used in connection with the Services, or (viii) export the Services in violation of applicable United States export Laws. Simple Security reserves the right to prevent or limit usage of the Platform and Services in excess of any limits imposed.

(e) Usage Limits. Access and use of the Services by Customer is subject to any usage limits set forth on the Order Form. Simple Security reserves the right to prevent or limit usage of the Platform in excess of such limits.

(f) Customer Users. The Platform will be accessed or used only by Users that are authorized to access the Platform using a user identifier and password provided to Customer by Simple Security or set up by Customer ("Users" and/or "Platform Users"). Customer will not make available the Platform to any person or entity other than Users. Customer will be responsible for the Users' compliance with the Agreement (including, without limitation, all license obligations, restrictions and limitations set forth in this Agreement) and for maintaining the confidentiality of all secure login information, passwords and other information related to its and its Platform users' respective accounts at all times.

2.2 IP Ownership. Simple Security and its licensors own and retain ownership in all right, title, and interest, including all intellectual property rights, in and to the Platform and the Services (including any modifications, enhancements, localizations or extensions thereto and including any Software), Simple Security Confidential Information, all information, technology, and other materials used by Simple Security (other than any data, technology, resources or materials provided by Customer or its licensors) to integrate the Services into the Customer systems (if applicable), and all intellectual property rights in each of the foregoing and any other materials or information in which Simple Security has ownership rights. The Services will be deemed and treated by Customer as Simple Security Confidential Information. Customer may from time to time, at its sole discretion, provide Simple Security with suggestions, comments or other feedback with respect to the use and operation of the Services ("Customer Feedback"). Customer agrees that any such Customer Feedback may be used and otherwise exploited by Simple Security for any reason without any obligation or payment to Customer.

2.3 Customer Data. Customer shall own and retain all right, title and interest, including all Intellectual Property rights, in and to all Customer Data. Customer hereby grants to Simple Security a worldwide, royalty-free, fully paid-up, non-exclusive, right and license during the Term to use, reproduce, modify, distribute, publicly display, and create derivative works of Customer Data for the purposes of (a) providing the Services, (b) the support and improvement of the Platform, (c) monitoring and resolving service, security, support or technical issues with the Services, and (d) as required in response to judicial or other governmental requests, subpoenas, warrants, and court orders, or as otherwise required by applicable law. Additionally, Simple Security may aggregate or de-identify Customer Data in a format such that neither Customer, its customers or any other person or household may be identified and use such aggregated or de-identified data for any lawful purposes, including to build and train Simple Security's machine-learning models and artificial intelligence algorithms.

2.4 Personal Information Processing. In connection with the Services, Simple Security will collect, use, retain and process Personal Information contained in Customer Data consistent with the Data Protection Addendum attached hereto as Exhibit A.

2.5 Suspension. Simple Security will have the right to suspend Customer's access to and use of the Services if Simple Security determines in its sole discretion that (a) Customer is engaged in activities that have resulted in or are likely to cause impairment of functionality of the Services for other customers , (b) there is a threat or attack on any of Simple Security's systems or services, (c) Customer's use of the Services disrupts or poses a security risk to Simple Security or to any other customer or vendor of Simple Security; (d) Customer is using the Services for fraudulent or illegal activities or in a manner that exceeds usage limitations; (e) Simple Security's provision of the Services to Customer is prohibited by applicable law, or (f) any vendor of Simple Security's has suspended or terminated Simple Security's access to or use of any third-party services, products, or technology reasonably required to enable Customer to access the Services. Simple Security will have

no liability for any damage, liabilities, losses (including any loss of use, loss of data, lost profits, or any business interruptions), or any other consequences that Customer may incur as a result of such a service suspension.

3. **Third Party Suppliers**. Customer acknowledges that certain features of the Services are delivered through or interoperate with third-party solutions, and Customer's use of such third-party solutions may be subject to the additional terms (the "Third Party Terms") to the extent expressly set forth in the Order Form. In such cases Customer accepts applicable Third Party Terms as a valid and enforceable written agreement and condition precedent to the use of the Services.

4. **Fees**.

4.1 Fees. Customer will pay to Simple Security the total fees as set forth on the Order Form, in accordance with any payment schedule set forth on the Order Form. All fees paid are non-refundable, provided, however, that if Customer terminates this Agreement or an Order Form for Simple Security's material breach that remains uncured after the applicable cure period, Simple Security shall refund any prepaid, unused fees for the terminated portion of the applicable subscription term, calculated on a pro rata basis.

If payment of any fees is not made when due and payable, a late fee will accrue at the rate of the lesser of one and one-half percent (1.5%) per month or the highest legal rate permitted by law and Customer will pay all reasonable expenses of collection. In addition, if any past due payment has not been received by Simple Security within thirty (30) days from the time such payment is due, Simple Security may suspend access to the Services until such payment is made.

4.2 Taxes. All amounts payable by Customer to Simple Security hereunder are exclusive of any sales, use and other taxes or duties, however designated (collectively "Taxes"). Customer will be solely responsible for payment of any Taxes, except for those taxes based on the income of Simple Security. Customer will not withhold any Taxes from any amounts due to Simple Security.

5. **TERM AND TERMINATION.**

5.1 Term and Termination.

(a) Term. Unless otherwise specified on the Order Form, this Agreement shall commence as of the Effective Date and shall continue for a period of one year unless earlier terminated as permitted hereunder (the "Term"). This Agreement will automatically renew for additional successive 1-year terms unless either party gives written notice of non-renewal at least thirty (30) days prior to the expiration of the then-current term.

(b) Termination. In addition to any other express termination right set forth in this Agreement:

(i) either Party may terminate this Agreement, effective on written notice to the other Party, if the other Party materially breaches this Agreement, and such breach: (A) is incapable of cure; or (B) being capable of cure, remains uncured thirty (30) days after the non-breaching Party provides the breaching Party with written notice of such breach; or

(ii) either Party may terminate this Agreement, effective immediately upon written notice to the other Party, if the other Party: (A) becomes insolvent or is generally unable to pay, or fails to pay, its debts as they become due; (B) files, or has filed against it, a petition for voluntary or involuntary bankruptcy or otherwise becomes subject, voluntarily or involuntarily, to any proceeding under any domestic or foreign bankruptcy or insolvency law; (C) makes or seeks to make a general assignment for the benefit of its creditors; (D) applies for or has appointed a receiver, trustee, custodian, or similar agent appointed by order of any court of competent jurisdiction to take charge of or sell any material portion of its property or business; or (E) if any change in federal or state laws and/or regulations make continued performance under this Agreement illegal or impossible.

(c) Effect of Expiration or Termination. Upon any expiration or termination of this Agreement: all licenses and rights granted to Customer hereunder will also expire or terminate, and (B) Customer shall cease all use of the Services, the Platform and Simple Security's Intellectual Property, and all copies thereof, in whole and in part, including in any production, marketing, distribution, licensing, sale, maintenance, support, or use of the Services, and uninstall any copies of Software from its systems.

(d) Survival. Any rights or obligations of the Parties in this Agreement which, by their nature, should survive termination or expiration of this Agreement will survive any such termination or expiration, including the rights and obligations set forth in this Section.

6. **CONFIDENTIALITY**.

6.1 Obligations. Simple Security and Customer each agree to hold each other's Confidential Information strictly confidential. Neither Simple Security nor Customer, unless required by Law, may use, disclose or otherwise make the other's Confidential Information available in any form to any third party (excluding its auditors, regulators, attorneys, accountants, and other third parties subject to similar confidentiality obligations) for any purpose other than to perform its obligations pursuant to this Agreement. Each Party shall ensure that (i) only personnel with a "need to access" Confidential Information in order to perform its contractual obligations to the other party will in fact have access to such Confidential Information, and (ii) Confidential Information is not disclosed or distributed by its employees or agents in violation of the terms of this Agreement. Each Party shall be responsible for any violation of the terms of this Section by its employees or agents. If either party is compelled by applicable laws, regulations or court orders to disclose any Confidential Information to any third party, that party will, except as prohibited by applicable laws, regulations or court orders, provide the other party with written notice of any such disclosure prior to any such disclosure.

6.2 Exceptions. Excluding non-public personal information, Confidential Information does not include information that: (a) is or becomes a part of the public domain through no act or omission of the other Party; (b) was in the other Party's lawful possession prior to the disclosure and had not been obtained by the other Party either directly or indirectly from the Disclosing Party; (c) is lawfully disclosed to the other Party by a third party without restriction on disclosure; or (d) is independently developed by the other Party without use of or reference to any Confidential Information of the Disclosing Party.

6.3 Return of Confidential Information. Upon the expiration or any termination of this Agreement, each Party shall promptly return, or if requested or return is not feasible, destroy and certify to such destruction, all Confidential Information and proprietary materials of the other Party, all copies thereof, and any summaries prepared (to the extent such summaries contain any of the other Party's Confidential Information) in its possession or under its reasonable control in accordance with applicable law. Notwithstanding the foregoing, each Party may retain one (1) copy of the other Party's Confidential Information for archival, legal and audit purposes; provided, however, that the confidentiality provisions of this Agreement shall apply to all such retained materials for so long as such Confidential Information (or any portion thereof) is in the possession or under the control of the Receiving Party.

6.4 Information Security Obligations. Each Party shall implement, and shall take measures to maintain, reasonable and appropriate administrative, technical, and physical security safeguards designed to: (i) ensure the security and confidentiality of Customer Data, Personal Information or Confidential Information of the other Party; (ii) protect against anticipated threats or hazards to the security or integrity of Customer Data, Personal Information or Confidential Information of the other Party; and (iii) protect against unauthorized access or use of Customer Data, Personal Information or Confidential Information of the other Party that could result in substantial harm or inconvenience to the other Party, a Customer or User.

6.5 Security Breach. In the event a party experiences a security breach which potentially or actually affects, directly or indirectly, Customer's Data or Confidential Information, such affected party will promptly, and in accordance with applicable laws: (i) notify other in writing; (ii) utilize commercially reasonable means to ensure that the security breach has ceased; (iii) investigate the nature, scope and duration of the breach and promptly provide other with details regarding the breach and cooperate and provide reasonable assistance with any remediation efforts undertaken by other; and (iv) notify

and cooperate with law enforcement, if applicable. Upon request the affected party will provide other with an update in writing on remediation actions.

7. **INDEMNIFICATION**.

7.1 Indemnification. If a third party makes a claim against either Customer or Simple Security ("Recipient" which may refer to Customer or Simple Security depending upon which party received the Material), that any information, design, specification, instruction, software, service, data, hardware, or material (collectively, "Material") furnished by either Customer or Simple Security ("Provider" which may refer to Customer or Simple Security depending on which party provided the Material) and used by the Recipient violates the third party's intellectual property rights, the Provider, at the Provider's sole cost and expense, will defend the Recipient against the claim and indemnify the Recipient from the damages, liabilities, costs and expenses awarded by the court to the third party claiming infringement or the settlement agreed to by the Provider, if the Recipient does the following: (a) notifies the Provider promptly in writing, not later than 30 days after the Recipient receives notice of the claim (or sooner if required by applicable law); (b) gives the Provider sole control of the defense and any settlement negotiations; (c) gives the Provider the information, authority and assistance the Provider needs to defend against or settle the claim.

7.2 If the Provider believes or it is determined that any of the Material may have violated a third party's intellectual property rights, the Provider may choose to either modify the Material to be non-infringing (while substantially preserving its utility or functionality) or obtain a license to allow for continued use, or if these alternatives are not commercially reasonable, the Provider may end the license for, and require return of, the applicable Material and refund any unused, prepaid fees the Recipient may have paid to the other party for such Material. If such return materially affects Simple Security's ability to meet obligations under a relevant Order, then Simple Security may, upon 30 day's prior written notice, terminate the Order.

7.3 The Provider will not be obligated to indemnify the Recipient to the extent that an infringement claim is based on the intentionally wrongful or illegal acts of the Recipient, a modification to any software or service performed by Recipient, any unauthorized use of any software, materials or service, or a combination with any third party or Recipient equipment, system, process or service where such combination was not reasonably anticipated given the nature of the Material and circumstances of furnishment and where such claim would not have arisen absent such combination.

7.4 This Section 7 provides the parties' exclusive remedy for any infringement claims or damages.

8. **REPRESENTATIONS AND WARRANTIES; DISCLAIMER**.

8.1 Simple Security Representations and Warranties. Simple Security represents and warrants that (a) it has the full power and authority to enter into this Agreement, to perform its obligations under this Agreement, and to grant the licenses and rights granted to Customer in this Agreement; (b) it will comply with all applicable Laws relating to its performance and/or obligations under this Agreement.

8.2 Customer Representations and Warranties. Customer represents and warrants that (a) it has the full power and authority to enter into this Agreement and to carry out its obligations under this Agreement; (b) upon execution and delivery of this Agreement by Customer, this Agreement shall be the legal, valid, and binding obligation of Customer, enforceable against it in accordance with the terms hereof; and (c) it will comply with all applicable Laws relating to its performance and/or obligations under this Agreement.

8.3 DISCLAIMER. EXCEPT AS EXPRESSLY STATED HEREIN, THE WARRANTIES SET FORTH IN SECTION 8.1 ARE LIMITED WARRANTIES AND ARE THE ONLY WARRANTIES MADE BY SIMPLE SECURITY HEREUNDER, INCLUDING WITH RESPECT TO THE SERVICES. EXCEPT AS OTHERWISE PROVIDED HEREIN SIMPLE SECURITY EXPRESSLY DISCLAIMS, AND CUSTOMER HEREBY EXPRESSLY WAIVES, ALL OTHER WARRANTIES OR REPRESENTATIONS WITH RESPECT TO THE SERVICES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, ERROR-FREE OPERATION, UNINTERRUPTED ACCESS, THAT THE SERVICES ARE SECURE, OR THAT THE SERVICES OR THE SOFTWARE WILL BE

AVAILABLE CONSTANTLY AND IN AN UNINTERRUPTED MANNER, AND ANY OTHER IMPLIED WARRANTY ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE.

8.4 THIRD PARTY PRODUCTS DISCLAIMER. SIMPLE SECURITY MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, AS TO ANY THIRD-PARTY PRODUCTS INCLUDING, WITHOUT LIMITATION, QUALITY, CAPABILITIES, OPERATIONS, PERFORMANCE, SUITABILITY MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT AND ALL OTHER WARRANTIES WITH RESPECT TO THIRD PARTY PRODUCTS ARE HEREBY EXPRESSLY DISCLAIMED. UNLESS OTHERWISE INDICATED, THIRD PARTY PRODUCTS PROVIDED UNDER THIS AGREEMENT ARE EXPRESSLY PROVIDED "AS IS."

9. **LIMITATION OF LIABILITY**.

9.1 UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, WILL SIMPLE SECURITY BE LIABLE TO CUSTOMER FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OF ANY KIND ARISING OUT OF THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, LOST PROFITS, LOST SALES OR BUSINESS, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOST DATA, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES, EVEN IF A REPRESENTATIVE OF SIMPLE SECURITY OR CUSTOMER HAS BEEN ADVISED, KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES. SIMPLE SECURITY WILL NOT BE LIABLE TO CUSTOMER UNDER THIS AGREEMENT FOR ANY DAMAGES, COSTS, OR LIABILITIES IN EXCESS OF THE FEES PAID BY CUSTOMER UNDER THIS AGREEMENT FOR THE TWELVE (12) MONTHS PRECEDING THE TIME OF ANY CLAIM. THIS LIMITATION OF LIABILITY IS CUMULATIVE AND NOT PER INCIDENT.

10. **GENERAL PROVISIONS**.

10.1 Complete Agreement. The Agreement (including the Order Form) contains the entire agreement of the Parties with respect to its subject matter and supersede all existing agreements and all other oral, written or other communications between them concerning its subject matter. No amendment to, or modification of, this Agreement shall be binding unless in writing and signed by a duly authorized representative of both Parties.

10.2 No Waiver. Failure by either Party to enforce any provision of this Agreement shall not be deemed a waiver of future enforcement of that, or any other, provision. Any waiver by either Party of its rights under this Agreement must be in writing and signed by a duly authorized representative of the waiving Party.

10.3 Assignment. Neither this Agreement nor any of the rights or obligations hereunder may be assigned by any party without the prior written consent of the non-assigning party. Any purported assignment without such consent shall be void and unenforceable. Notwithstanding the foregoing either Party has the right to assign and transfer this Agreement, and its rights and obligations, to any affiliate and otherwise in connection with a sale or transfer of all or substantially all of its business or assets to which this Agreement relates, whether by sale of stock or assets, merger, operation of the law, or otherwise. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective successors and permitted assigns.

10.4 Headings. Headings and subheadings are for convenience only and shall not be deemed to be a part of this Agreement.

10.5 Severability. In the event that any provision of this Agreement conflicts with the law under which this Agreement is to be construed or if any such provision is held illegal, invalid or unenforceable by a court of competent jurisdiction (a) such provision shall be deemed to be restated to reflect as nearly as possible the original intentions of the parties in accordance with applicable Law; and (b) the remaining terms, provisions, covenants and restrictions of this Agreement shall remain in full force and effect.

10.6 Independent Contractor. The Parties hereto are independent contractors, and nothing herein shall be construed to create any other relationship between them.

10.7 Equitable Relief. Each Party shall be entitled to seek injunctive or other equitable relief whenever the facts or circumstances are such that the Party seeking such relief shall have no adequate remedy at law. A Party's right to seek equitable relief pursuant to this Section will not prohibit that Party from pursuing any other remedies, including the recovery of damages.

10.8 Governing Law and Venue. This Agreement shall be governed by and construed in accordance with the laws of the state of Florida. The state and federal courts located in Florida shall be the exclusive venue for, and have exclusive venue jurisdiction over, the Parties hereto with respect to any matter arising out of or relating to this Agreement, and the Parties hereby submit to such courts' jurisdiction over the Parties with respect to any matter arising out of or relating to this Agreement. Each Party hereby irrevocably waives, to the fullest extent permitted by law, any objection which it may now or hereafter have to the jurisdiction and laying of the venue of any such proceeding brought in such a court and any claim that any such proceeding brought in such a court has been brought in an inconvenient forum. No part of this Agreement shall be construed against a Party because that part or any part was drafted or revised by or on behalf of such Party.

10.9 Notices. All legal notices, reports, approvals or consents required or permitted under this Agreement ("Communications") between the parties shall be in writing and shall be deemed given when: (a) delivered personally; (b) five (5) days after having been sent by registered or certified mail, return receipt requested, postage prepaid; or (c) one (1) day after deposit with a commercial overnight carrier specifying next day delivery, with written verification of receipt. All Communications shall be sent to the respective addresses set forth in the preamble or to such other address as may be designated by a Party by giving written notice to the other Party.

10.10 Force Majeure. Neither Party shall be deemed to have breached this Agreement because of any delay or failure in its performance arising from events beyond its reasonable control, including, but not limited to, acts of God, acts of war, riot, epidemic, fire, flood or other disasters ("Force Majeure"), provided that financial inability in and of itself will not be a Force Majeure event.

10.11 Counterparts. The Agreement may be executed in one or more counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument. Execution and delivery of this Agreement electronically is hereby deemed valid and effective; a signed facsimile, PDF, or electronic copy is hereby deemed an original for all purposes; and the Parties fully intend that each may rely upon such signature as being a true signature of the Party's authorized officer or representative and deemed as due execution and delivery for all purposes whether or not hard copies of this Agreement were or are ever exchanged between them.

10.12 Survival of Obligations. Obligations and rights that, by their nature, are intended to survive termination or expiration of this Agreement shall so survive.

[Remainder of this page intentionally left blank; signature page follows.]

IN WITNESS WHEREOF, the Parties, intending to be legally bound hereby, have each caused its duly authorized officers or representatives to execute this Agreement as of the Effective Date.

SIMPLE SECURITY INC		**[CUSTOMER NAME]**	
By:	_____	By:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

EXHIBIT A

DATA PROTECTION ADDENDUM

1.0 This Data Protection Addendum (this "DPA") applies to Simple Security's processing of Personal Information received from Customer for the purposes of Simple Security's performance of the Services under the Agreement. In the event of a conflict between any provisions of the Agreement and the provisions of this DPA, the provisions of this DPA shall govern and control.

2.0 **Consumer Privacy Laws and Regulations**. Simple Security acknowledges that data transmitted by Customer to Simple Security in connection with the Services may be subject to consumer privacy laws and regulations, as well as common law restrictions and/or obligations (the "Consumer Privacy Laws"). Consumer Privacy Laws may include, but is not limited to, laws, and associated regulations or guidance, such as pursuant to the California Consumer Privacy Act (the "CCPA") and California Privacy Rights Act ("CPRA", as codified in California Civil Code sections 1798.100, et seq., (collectively, "CCPA/CPRA"), the Virginia Consumer Data Privacy Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and other similar laws currently in effect or that may come into effect during the term of the Agreement, all as applicable and as may be amended from time to time.

3.0 **Relationship**. Based on Simple Security's relationship with Customer in connection with the Services, Simple Security may be considered a "service provider," "contractor," or "processor" (collectively, "Processor") under the Consumer Privacy Laws in connection with the performance of the Services. As a Processor, in performing the Services Simple Security may process and/or receive "personal information" or "personal data," as such terms are defined in applicable Consumer Privacy Laws, from, or on behalf of, Customer (such personal information or personal data is herein referred to as "Personal Information"). Personal Information will include all such personal information contained in Customer Data as defined in the Agreement.

4.0 **Simple Security Requirements.** Simple Security will adhere to the following requirements pursuant to its performance of the Services:

4.1 Simple Security will comply with all of Customer's lawful instructions regarding the processing of Personal Information.

4.2 Simple Security will not "sell" or "share," as defined by applicable Consumer Privacy Laws, Personal Information.

4.3 Customer is providing Simple Security access to Personal Information for the limited and specific purposes provided in Section 6.1 of this DPA, and/or as otherwise expressly permitted by Consumer Privacy Laws. Simple Security shall not retain, use, or disclose Personal Information for any other purpose(s).

4.4 Simple Security shall not retain, use, or disclose Personal Information for any "commercial purpose" other than the Customer's purposes specified in Section 6.1 of this DPA.

4.5 Simple Security shall not retain, use, or disclose Personal Information outside of the direct relationship between Simple Security and Customer.

4.6 Simple Security shall not combine or update Personal Information with any other information, except as provided for under Consumer Privacy Laws.

4.7 Simple Security shall comply with all applicable laws and obligations regarding the use and protection of Personal Information, including all Consumer Privacy Laws.

4.8 Simple Security shall assist the Customer in meeting the Customer's obligations in relation to the Personal Information and protect the Personal Information as follows:

i. processing Personal Information solely to the extent the processing is necessary, reasonable, and proportionate to the specific purpose(s) listed in Section 6.1 of this DPA or otherwise permitted by Consumer Privacy Laws;

ii. cooperating with Customer in responding to and complying with verifiable consumer requests made pursuant to Consumer Privacy Laws, insofar as this is possible;

iii. implementing reasonable security procedures and practices to protect the Personal Information from unauthorized or illegal access, destruction, use, modification, or disclosure while in possession of Simple Security in accordance with California Civil Code section 1798.81.5 and other states' similar requirements, including but not limited to technical and organizational measures appropriate to the nature of the Personal Information and risk to the same; and

iv. providing notification of any actual Security Event related to any system, platform, or process that Simple Security and its employees or contractors use to process Personal Information.

4.9 For purposes of this DPA, a "Security Event" means an unauthorized access or acquisition of Personal Information, or circumstances that Simple Security reasonably determines would place Personal Information at risk. To assist Customer in relation to any Personal Information breach notifications it is required to make, Simple Security shall report any actual Security Event to Customer without undue delay.

4.10 If Simple Security receives any subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority, which relates to the processing of Personal Information ("Disclosure Request"), it will promptly pass on such Disclosure Request to Customer, unless otherwise required by applicable law. Simple Security expressly reserves the right to respond to such Disclosure Request as it deems reasonably appropriate.

4.11 Simple Security shall ensure that each person processing Personal Information is subject to a duty of confidentiality with respect to such Personal Information.

4.12 If Simple Security engages any other person or entity to assist it in processing Personal Information for purposes of providing the services enumerated in the Agreement, to the extent required by law Simple Security shall: (a) provide Customer with the opportunity to object to that proposed engagement at least five day(s) in advance; and (b) ensure that the engagement complies with all Consumer Privacy Laws and is pursuant to a written contract binding such party to observe all requirements regarding Personal Information and Customer's rights in relation to the same, as laid out herein.

4.13 Unless otherwise required by law, Simple Security will delete and destroy Personal Information, and all copies of the same, by using the secured deletion capability provided by the Third Party Hosting Provider (defined below) to delete the virtual machines, databases and other resources used to process Personal Information for Customer upon expiration or termination of the applicable Order.

4.14 Upon the reasonable request of Customer, Simple Security shall make available to Customer all information necessary to demonstrate Simple Security's compliance with all Consumer Privacy Laws or to enable Customer to conduct and document any required data protection assessments.

4.15 Simple Security shall notify Customer if Simple Security determines it can no longer meet any of its Consumer Privacy Laws obligations.

5.0 **Data Processing and Security.** During processing of Personal Information for the purposes of the Services, Simple Security will maintain Personal Information in a secure fashion aligned with industry standards for the management and

processing of private consumer information. Simple Security shall be responsible for providing industry standard system and data security in connection with the Platform and services and will use commercially reasonable efforts to prevent unauthorized access to or the creation of any unauthorized copies of any Personal Information in any form.

6.0 **Description of Processing**.

6.1 Nature and Purpose of Processing. The processing of Personal Information is for the following Customer purposes related to the Services, in accordance with the Agreement:

i. Short-term, transient use, provided that the individual's Personal Information is not disclosed to another third party and is not used to build a profile about the individual or otherwise alter the individual's experience outside the current interaction with the Customer.

ii. Performing services on behalf of the Customer, including providing analytics and cybersecurity services, or providing similar services on behalf of the Customer.

6.2 Type of Data Involved in Processing. Depending on how the Customer chooses to use the Services and the additional services subscribed by Customer, Simple Security may process the following types of Personal Information:

i. Data related to Customer's Users: Personal Information of the Users of a Customer, including name, address, email address, mobile number, and transactional information, location and time where an order took place, IT information (location data, IP address, cookie ID, etc.) and marketing, product, and other preference information.

ii. Data related to representatives: Personal Information of representatives of Customer, including name, business contact information, username, and password and IT information (location data, IP address, cookie ID, etc.).

6.3 Duration of Processing. Simple Security shall process Personal Information until the date of expiration or termination of performance of the Services, unless instructed otherwise by Customer.

7.0 **Additional Terms**.

7.1 Third Party Hosting Providers. Simple Security may utilize third party hosting providers to provide the Services (a "Third Party Hosting Provider"). Customer acknowledges and agrees that Simple Security may use Amazon Web Services ("AWS") or an equivalent Third Party Hosting Provider as a sub-processor. Customer further understands and agrees that Simple Security is subject to standard terms and conditions with respect to such commercial arrangements, and expressly approves the standard agreement with such Third Party Hosting Providers as a sub-processor agreement.

7.2 Right to Monitor. Simple Security grants Customer the right to take, and Simple Security shall allow and contribute to, appropriate and reasonable steps to monitor so as to ensure Simple Security's use of Personal Information in connection with the Services is consistent with all privacy rights and obligations, whether statutory, regulatory, based in common law, contractual, or otherwise.

7.3 Right to Remediate. Simple Security grants Customer the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information.

7.4 Disputes. Any disputes arising from or in connection with this DPA shall be brought as set forth in the Agreement.

8.0 **Transfers to Third Countries.** This section applies to the extent Personal Information is furnished by one Party to the other that originates from a member country of the EU or the European Economic Area (EEA), the United Kingdom (UK), Switzerland, or another jurisdiction subject to data protection laws based on the European Union General Data Protection Regulation ("GDPR").

8.1 Simple Security shall maintain an up-to-date list of sub-processors and make such list available to Customer and update it with details of any new sub-processors and shall notify Customer in advance of such new sub-processor processing Customer Personal Information. Simple Security shall notify Customer of any intended changes concerning the addition or replacement of sub-Processors to the list of sub-processors set forth in Schedule 2 in accordance with Section 4.12 of this DPA.

8.2 To the extent that any Personal Information originating from the EEA or Switzerland is transferred (including by way of remote access) to a jurisdiction not recognized by the European Commission as providing an adequate level of data protection, the Parties agree that the EU Standard Contractual Clauses set forth in Commission Implementing Decision (EU) 2021/914 (the "SCCs") are hereby incorporated by reference and form part of this DPA. The applicable module of the SCCs shall apply based on the role of the Parties in the relevant processing activity, including Module One (controller to controller), Module Two (controller to processor), Module Three (processor to processor), and, where applicable, Module Four (processor to controller). In the event of any conflict between the module identified in the Schedules and the actual roles of the Parties, the module reflecting the Parties' actual roles shall control. For the purpose of the SCCs:

A. Clause 7: the optional docking clause shall apply;
B. Clause 9 (not applicable to Module One): Option 2 (General Written Authorization) shall apply. The time period for prior notice of intended sub-processor changes shall be as set out in Section 4.12 of this DPA;
C. Clause 11: the optional language shall not apply;
D. Clause 17: governing law shall be the law of an EU Member State that allows for third-party beneficiary rights, which shall be the laws of the Netherlands, unless otherwise selected by the data exporter;
E. Clause 18(b): disputes will be resolved before the courts of the Netherlands;
F. Schedule 1 of this DPA shall serve as Annex I of the SCCs, and Schedule 2 of this DPA shall serve as Annex II of the SCCs.

The Parties shall comply with their respective obligations under the SCCs, including implementing appropriate technical and organizational measures and assessing, on an ongoing basis, whether the laws and practices of the destination country affect compliance with such clauses.

8.3 To the extent that any Personal Information originating from the United Kingdom is transferred (including by way of remote access) to a jurisdiction not recognized as providing an adequate level of protection under UK data protection law, the Parties agree that the UK International Data Transfer Addendum to the SCCs (the "UK Addendum") is hereby incorporated by reference and forms part of this DPA. The UK Addendum shall apply to the SCCs as incorporated herein and shall be deemed completed with the information set forth in this DPA and the Schedules. The applicable module shall correspond to the roles of the Parties as described in this DPA. In the event of any conflict between the SCCs and the UK Addendum, the UK Addendum shall prevail with respect to Personal Information originating from the United Kingdom.

8.4 Each party shall comply with its respective obligations under applicable Data Protection Law in connection with the processing of Personal Information under this DPA. The Parties agree to cooperate in good faith to promptly

execute any additional agreements to ensure their compliance with international transfers of Personal Data as required by Data Protection Law.

8.5 The schedules, as applicable to the appropriate module, attached to this DPA are incorporated herein and made part of this DPA and the Agreement.

Schedule 1 to the Data Protection Addendum

Description of Transfer

Selected Module for SCCs: Module Two

The categories of data subjects, categories of personal data, nature and purpose of processing, and duration of processing are as described in Section 6 of this DPA.

For clarity and for purposes of Annex I of the Standard Contractual Clauses:

- ***Categories of data subjects:*** *as described in Section 6.2*
- ***Categories of personal data:*** *as described in Section 6.2*
- ***Nature and purpose of processing:*** *as described in Section 6.1*
- ***Duration of processing:*** *as described in Section 6.3*

Schedule 2 to the Data Protection Addendum

List of Sub-Processors

(Not applicable to Module One of the SCCs)

Controller generally authorizes the engagement of sub-processors and specifically consents to those identified by Simple Security to Customer as updated from time to time.

Schedule 3 to the Data Protection Addendum

SCCs Appendix

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: _____
Address: _____
Contact person's name, position and contact details:
_____

Activities relevant to the data transferred under these Clauses: See Agreement and Schedule 1.

Role (controller/processor): Controller

Data importer(s):

Name: Simple Security Inc.
Address: 7901 4th St. N., Suite 23478, St. Petersburg, FL 33702

Contact person's name, position and contact details:
Steve Hindle; Privacy Officer; steve.hindle@simple.security

Activities relevant to the data transferred under these Clauses: See Agreement and Schedule 1.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

See Schedule 1.

C. COMPETENT SUPERVISORY AUTHORITY

If Customer is the exporter:

The supervisory authority shall be determined in accordance with Clause 13 of the Standard Contractual Clauses based on the location of the data exporter.

ANNEX II

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

Data Importer maintains and enforces industry standard technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and ensure a level of security appropriate to the risk of its processing of personal data processing consistent with its obligations under the master

services agreement and applicable privacy laws. These measures shall include a comprehensive information security program that includes administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of personal data that are appropriate to the type of information that Data Importer will process. Data Importer shall regularly monitor compliance with these safeguards.

To mitigate the risk to information processing resources, unauthorized disclosure or erasure of information and interruption of support for business processes which may result from unauthorized access, security controls implemented by the Data Importer are included in the following sections:

- *Organizational Control – Measures which comply with the specific requests of data protection, regarding the internal organization such as commitment of employees to data secrecy, data backup/deletion, spatial/personal separation of data from other clients etc.*
- *Entry Control – Measures to limit entrance of unauthorized persons to areas where personal data is used or processed such gate control, identification badges/code cards etc.*
- *Admission Control – Measures to limit admission of unauthorized persons to systems where personal data is used or processed such as safeguarding of physical network infrastructure, firewalls etc.*
- *Access Control – Measures to limit access of unauthorized persons to systems where personal data is used or processed such as having least privilege/selective access policy, use of encryption, audit logging, individual user ids/strong passwords, regulated procedures for granting, changing and revocation of access rights etc.*
- *Transmission Control – Measures to ensure that personal data cannot be read, copied, modified or removed without authorization such as use of encryption both at rest and in transit, audit logging to have retrospect information which data has be retrieved by whom etc.*
- *Availability Control – Measures to ensure that personal data is protected from accidental destruction or loss such as fail over capabilities, regular tested backups stored in multiple locations and disaster recovery plan, change management process etc.*
- *Separation Control – Measures to ensure that data collected for different purposes can be processed separately such use of separate user roles, logical/physical separation of data etc.*

ANNEX III
LIST OF SUB-PROCESSORS

See Schedule 2.

ANNEX IV
ADDITIONAL PROVISIONS REGARDING THE FEDERAL ACT ON DATA PROTECTION OF 19 JUNE 1992

The Parties agree to the following provisions regarding the rights of data subjects pursuant to the Swiss Federal Act on Data Protection of 19 June 1992:

1. The term "member state" as used in these Clauses shall not be interpreted by the Parties in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in according with Clause 18(c).

2. These Clauses shall be interpreted to protect the data of legal entities afforded data protection and data privacy rights under the Swiss Federal Act on Data Protection of 19 June 1992 until such time as the revised Swiss Federal Act on Data Protection of 25 September 2020 enters into effect.