MASTER SERVICES AGREEMENT

This Master Services Agreement is made by and between Riskonnect Active Risk Ltd, with its principal office located at 3rd Floor, 70 Gracechurch Street, London, EC3V 0XL, United Kingdom and its Affiliates (collectively, "**Riskonnect**") and [•] , having its principal place of business at [•] ("**Customer**"). Hereinafter, Riskonnect and Customer may individually be referred to as a "Party" and may collectively be referred to as the "Parties".

This Master Services Agreement consists of this signature page, the attached General Terms and Conditions and the following attached schedules ("**Schedules**") and Exhibits ("**Exhibits**") that are listed below:

Schedule A:	Product Schedule(s), as applicable
Schedule B:	AI and Data Usage Product Schedule, if applicable
Exhibit A:	Initial Statement of Work(s)
Exhibit B:	Initial Subscription Order
Exhibit C:	Security Exhibit(s)
Exhibit D:	Data Processing Addendum

By executing this Agreement, the Parties confirm that they have reviewed and fully understand its contents, including the General Terms and Conditions, as well as the Schedules and Exhibits referenced above, all of which are incorporated by reference. The Parties agree to be legally bound by the terms herein. This Agreement shall be executed by their respective duly authorized representatives and will take effect as of the date of the last signature below. (the "**Effective Date**").

Customer		Riskonnect Affiliate	
[Customer Name]		**Riskonnect Active Risk Ltd**	
Signature:	_____	Signature:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

GENERAL TERMS AND CONDITIONS

1. DEFINITIONS

The capitalized terms used in this Agreement, and not defined elsewhere within this Agreement, shall have the meanings specified below.

1.1 "**Affiliate**" means with respect to a Party, any entity that directly or indirectly, through one or more intermediaries, controls, is controlled by or is under common control with that Party. The term "**Control**" (including the terms "controlled by" and "under common control with") means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such entity, organization or body, whether through the ownership of voting securities or otherwise.

1.2 "**Agreement**" means, collectively:

1.2.1 this Master Services Agreement; and

1.2.2 any applicable subsequent Statement of Work, Subscription Order, or Project Change Order; and

1.2.3 any Supplemental Materials; and

1.2.4 other documents, attachments and addenda that the Parties' authorized representatives may mutually agree to in writing from time to time.

1.3 "**Annual Services**" means services, other than Software Support, provided to Customer, such as maintenance change requests, training, data services, modification of data interfaces, managed services, and other services, as set forth in the applicable Subscription Order.

1.4 "**Business Day**" means a day other than a Saturday, Sunday or public holiday, on which clearing banks are open for non-automated commercial business in the City of London.

1.5 "**Confidential Information**" means all confidential and proprietary information disclosed by a Party to the other Party, whether orally, in writing, or electronically, that is either explicitly designated as confidential or that, given the nature of the information and the circumstances of its disclosure, a reasonable person would conclude is intended to be treated as confidential. This includes, but is not limited to, information that is shared in a secure setting or accompanied by oral or written remarks indicating its confidentiality. This includes, but is not limited to:

1.5.1 business and marketing plans, identity of clients or prospective clients; and business processes;

1.5.2 technology and technical information, product designs, software, source code and object code, screenshots, data models, data conversion and processing logic, formulae and processes, know-how, and show-how;

1.5.3 discoveries, inventions, developments, improvements, works of authorship, concepts, mask works, and ideas, or expressions thereof, whether subject to patents, copyright, trademark, trade secret protection or other intellectual property right protection (in the United States or elsewhere) and whether in tangible or intangible form and whether or not stored, compiled or memorialized physically, electronically, graphically, photographically or in writing;

1.5.4 the terms and conditions of this Agreement (including pricing), Customer Data, and the Riskonnect Service.

Confidential Information (except for Customer Data) shall NOT include any information that is or becomes generally known to the public without breach of any obligation owed to the other Party; was known to a Party prior to its disclosure by the other Party without breach of any obligation owed to the other Party; was independently developed by a Party without breach of any obligation owed to the other Party; or is received from a third party without breach of any obligation owed to the other Party.

1.6 "**Customer Data**" means the information or material, including Customer's Confidential Information and Personal Data, that Customer and Users submit, upload, or transfer, or cause to be submitted, uploaded, or transferred to the Customer's configuration of the Riskonnect Application. For clarity, Customer Data shall not include de-identified or aggregated data.

1.7 "**Data Protection Laws and Regulations**" encompass all laws and regulations that govern the processing, as that term is defined by applicable laws and regulations, of Personal Data in connection with this Agreement. This includes, but is not limited to, regulations pertaining to individual privacy rights, data security measures, and cross-border data transfers, as enforced by relevant authorities. For the purposes of this Agreement, the laws specific to China and Russia are expressly excluded.

1.8 "**Disabling Code**" means any programming devices (e.g., viruses, key locks, back doors, trap doors, etc.) which would (i) disrupt the use of a Riskonnect Application or any system, equipment or software to which Customer's networks are interfaced or connected; or (ii) destroy or damage data or make data inaccessible or delayed, except for file and purge routines necessary to the routine maintenance of a Riskonnect Application or other mechanisms to monitor Customer's compliance with the terms of this Agreement.

1.9 "**Documentation**" means, in Web-based form, any manuals, user guides, technical specification documents and other instructional and reference materials generally distributed by Riskonnect regarding the Riskonnect Applications, all as updated and redistributed by Riskonnect from time to time.

1.10 "**Intellectual Property Rights**" shall mean all copyright, patent, trademark, trade secret and other intellectual property and proprietary rights.

1.11 "**Licensor**" means a third-party provider of products or services to Riskonnect necessary for Riskonnect to provide the Riskonnect Service, as set forth in the applicable Product Schedule, SOW, or Subscription Order.

1.12 "**Modeling and Analytics Services**" means modeling and/or business analytics services, including hazard loss and catastrophe modeling, loss forecasting and triangles, adverse event simulation, scenario and portfolio risk analysis, decision mapping, risk bearing and risk retention tolerance analysis and insurance program evaluation analysis.

1.13 "**Non-Riskonnect Service Application**" means a third-party or Customer-implemented product, service or application unrelated to or integrated with the Riskonnect Service.

1.14 "**Personal Data**" means any data or other information that relates to an identified or identifiable individual, or as otherwise defined under Data Protection Laws and Regulations.

1.15 "**Product Schedule**" means the additional terms applicable to the Riskonnect Service(s) licensed to Customer under this Agreement. The initial Product Schedule(s) is/are attached hereto as **Schedule A**.

1.16 "**Professional Services**" means any consulting, training, implementation, configuration, Annual Services, Software Support, or other professional services provided by Riskonnect and paid by Customer pursuant to the Agreement, including an applicable Statement of Work.

1.17 "**Project Change Order**" or "**PCO**" means a document (including any exhibits or attachments) on a form issued by Riskonnect signed by both Parties that specifies one or more changes to the Professional Services to be provided by Riskonnect to Customer under a Statement of Work, and which may include changes to the objectives, scope of work, initial implementation deliverables, and/or fees with respect to such Professional Services.

1.18 "**Riskonnect Application**" means the Web-based version of the proprietary computer software programs of Riskonnect, as configured for Customer by Riskonnect, and all improvements, updates, licensed internal code, embedded third-party software, upgrades, new versions, modifications, subsequent releases, fixes, enhancements, derivative products and information used by Riskonnect in providing Customer access to the Riskonnect Service, as further described in **Schedule A** and as identified in an applicable Subscription Order.

1.19 "**Riskonnect Service**" means, collectively, (i) the Riskonnect Application; (ii) Licensors' proprietary technology (including audio and visual information, documents, software, hardware, products, methods, processes, algorithms, user interfaces, know-how, techniques, designs and other tangible or intangible technical material or information); and (iii) any deliverables set forth in each Statement of Work, Subscription Order, and/or addendum.

1.20 "**Software Support**" means support services, other than Annual Services, provided to Customer for password resets, software errors, minor bug fixes, or other support services, as more fully described in Riskonnect's Service Level Agreement found at https://riskonnect.com/legal-sla/.

1.21 "**Statement of Work**" or "**SOW**" means a document (including any exhibits or attachments) on a form issued by Riskonnect signed by both Parties that specifies the Professional Services to be provided by Riskonnect to Customer, and which may include objectives, scope of work, initial implementation deliverables, and/or fees with respect to such Professional Services. The initial Statement of Work is attached hereto as **Exhibit A**.

1.22 "**Subscription Order**" or "**Order**" means a document on a form issued by Riskonnect signed by Customer that specifies the Riskonnect Applications and other subscriptions ordered by Customer and the associated fees for such subscriptions. The initial Subscription Order or Order is attached hereto as **Exhibit B**.

1.23 "**Supplemental Materials**" means the following documents, provisions or materials either available at a link set forth below or attached to this Agreement, all of which are incorporated into the Agreement by reference:

1.23.1 Riskonnect Privacy Notice available at http://riskonnect.com/privacy-notice;

1.23.2 Data Transfer Protocols as applicable, available at https://riskonnect.com/legal-dtps/;

1.23.3 Riskonnect Security Exhibit attached as **Exhibit C**; and

1.23.4 Other materials as may be set forth in a document signed by the Parties.

During the Term, Riskonnect may not materially modify or degrade any obligation set forth in the Supplemental Materials without Customer's consent.

1.24 "**Term**" means the period from the Effective Date until (i) all Subscription Orders hereunder have expired or been terminated, or (ii) the Agreement has been terminated in accordance with Section 8.

1.25 "**User**" means an individual, including Customer's employees, representatives, agents or third parties employed or retained by Customer to perform services for or on behalf of Customer, who are authorized by Customer to use or access Customer's configuration of the Riskonnect Service and whom have been issued a User-ID or who otherwise access or use the Riskonnect Service.

1.26 "**User-ID**" means a unique user identification and password provided or assigned to a User.

2. RIGHT TO USE THE RISKONNECT SERVICE; RESTRICTIONS

2.1 **User Access**. Subject to the terms and limitations set forth in this Agreement, Riskonnect hereby grants to Customer a limited term, revocable, worldwide, non-exclusive, non-sublicensable, non-transferable (except as set forth in Section 14.1), right and license for Users to use Customer's configuration of the Riskonnect Service, subject to any restrictions in a Subscription Order, solely for Customer's own internal business purposes. Customer shall provide the equipment and software (including obtaining any third-party software licenses) required to access the Riskonnect Service in accordance with, and to otherwise comply with, the hardware/software specifications for the Riskonnect Service. Customer shall be responsible for all maintenance and compliance with laws, if applicable, of Customer networks, equipment and system security required or appropriate in connection with the Riskonnect Service.

2.2 **Reserved Rights**. All rights not expressly granted to Customer are reserved by Riskonnect and its Licensors and no implied licenses are granted.

2.3 **Restrictions**. Customer shall not, and shall not permit any third party (including Users) to:

2.3.1 license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, timeshare, provide on a service bureau basis or otherwise commercially exploit or make available the Riskonnect Service to any third party;

2.3.2 modify, copy or make a derivative work based upon the Riskonnect Service or any part of the services of Riskonnect's Licensors;

2.3.3 create Internet "links" to the Riskonnect Service, any part of the services of Riskonnect's Licensors, or "frame" or "mirror" the Riskonnect Service other than on Customer's own intranets or otherwise for Customer's own internal business purposes;

2.3.4 reverse engineer or access the Riskonnect Service, or any part of the services of Riskonnect's Licensors, in order to develop a competitive product or service, develop a product using similar ideas, features, functions or graphics of the Riskonnect Service, or copy any ideas, features, functions or graphics of the Riskonnect Service;

2.3.5 use or access the Riskonnect Service in a manner, or act otherwise in any manner, that could damage, disable, overburden, or impair any Riskonnect servers, or the networks connected to any Riskonnect server;

2.3.6 interfere with or disrupt the integrity or performance of the Riskonnect Service or the data contained therein, or any third party's use and enjoyment thereof;

2.3.7 attempt to gain unauthorized access to the Riskonnect Service, accounts, computer systems, or networks connected to any Riskonnect server through hacking, password mining, or any other means;

2.3.8 use or access the Riskonnect Service to send spam or otherwise duplicative or unsolicited messages in violation of applicable laws;

2.3.9 use or access the Riskonnect Service to send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material that is harmful to children or violates third-party privacy rights; or

2.3.10 use or access the Riskonnect Service to send or store viruses, worms, time bombs, Trojan horses or other harmful or malicious code, files, scripts, agents or programs.

3. USERS

3.1 **User-IDs**. Customer acknowledges and undertakes to ensure that no User will use or share the User-ID of any other User. Customer will safeguard the User ID's and other security data and methods furnished to Customer in connection with the Riskonnect Service and prevent unauthorized access to or use of the Riskonnect Service. Customer shall notify Riskonnect if it becomes aware of any unauthorized access or use of the Riskonnect Service. No User shall be engaged in the business of providing software or software-as-a-service for the management of risk, claims or compliance matters.

3.2 **Customer Responsibility for Users**. Customer is responsible for all Users and the activity occurring under Customer's User accounts and shall abide by all applicable local, state, national and foreign laws, treaties and regulations in connection with Customer's use of the Riskonnect Service in accordance with the terms of this Agreement, including those related to data privacy, international communications and the transmission of technical, financial or personal data.

3.3 **Riskonnect Licensors**. Customer's subscription does not include a subscription to use applications provided directly by Riskonnect's Licensors outside of the Riskonnect Service.

3.4 **Reserved Rights**. Riskonnect reserves the right to immediately suspend access under any User ID which Riskonnect reasonably suspects poses a risk to the security of Customer Data or the Riskonnect Service, or which Riskonnect reasonably suspects of activity that is in material breach of the terms of this Agreement.

4. DATA; PRIVACY AND SECURITY; AI

4.1 **Customer Owns Customer Data**. Customer owns all right, title and interest in and to the Customer Data, which shall never be deemed to be the Riskonnect Service, even if delivered or incorporated therewith. Customer shall have sole responsibility, and Riskonnect shall have no responsibility whatsoever, for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership of Customer Data, and Riskonnect shall not review, monitor or check the Customer Data except as instructed by Customer or as otherwise necessary to provide the Riskonnect Service to Customer. Riskonnect shall have no liability for the deletion, destruction, damage or loss of any Customer Data by Users, or through no fault of Riskonnect or its Licensors, without limiting Riskonnect's obligations to comply with its data backup practices.

4.2 **Safeguards**.

4.2.1 Riskonnect shall maintain and handle all Customer Data with commercially reasonable physical, electronic, and procedural safeguards to protect and preserve the confidentiality and security of Customer Data in accordance with (1) applicable data protection laws and regulations; (2) the Riskonnect Security Exhibit; (3) Riskonnect Privacy Notice set forth in the Supplemental Materials, and (4) the applicable data processing addendum attached hereto as Exhibit D.

4.2.2 Riskonnect shall not license, transmit or disclose Customer Data to any third party, except to (i) Riskonnect's and Affiliates' employees and contractors who are subject to written confidentiality requirements no less restrictive than those contained herein, (ii) Riskonnect Licensors, (iii) as required by applicable law, regulation or rule, and (iv) Users.

4.2.3 Regardless of location of storage or access of Customer Data, Riskonnect and Affiliate employees and contractors will deploy the same data protection safeguards in compliance with the terms and conditions of this Agreement and in compliance with Data Protection Laws and Regulations.

4.2.4 Riskonnect will not sell Customer Data to any third party.

4.3 **Artificial Intelligence**. If Customer licenses an AI Feature (as defined in **Schedule B**) from Riskonnect, each Party agrees to comply with the terms set forth in Schedule B.

4.4 **Integration of Non-Riskonnect Service Applications**. If Customer acquires, licenses or otherwise obtains a Non-Riskonnect Service Application, any exchange of data between Customer and any third-party provider of a Non-Riskonnect Service Application is solely between Customer and such third party. Riskonnect provides no warranties or support for Non-Riskonnect Service Applications.

5. CONFIDENTIALITY

5.1 **Standard of Care**. Each Party acknowledges and agrees that during the Term it may be furnished with or otherwise have access to Confidential Information of the other Party. A Party receiving Confidential Information ("**Receiving Party**"), from the Party disclosing Confidential Information ("**Disclosing Party**"), shall exercise the same degree of care and protection that it exercises with respect to its own Confidential Information, but in no event shall Receiving Party exercise less than a reasonable standard of care. Receiving Party shall only use, access and disclose Confidential Information as necessary to fulfill its obligations or in exercise of its rights expressly granted under this Agreement. Receiving Party shall not directly or indirectly disclose, sell, copy, distribute, republish, create derivative works from, demonstrate or allow any third party to access any of Disclosing Party's Confidential Information; provided, however, that:

5.1.1 Receiving Party may disclose Disclosing Party's Confidential Information to Receiving Party's Affiliates, employees, Licensors, and other agents who have a need to know; and

5.1.2 All use of the Disclosing Party's Confidential Information shall be subject to all the restrictions set forth in this Agreement; and

5.1.3 Receiving Party may disclose Confidential Information that is not Customer Data or the Riskonnect Application to attorneys, agents and consultants who need to know the Confidential Information to enable such Party to perform under this Agreement and who have previously agreed to be bound by confidentiality obligations no less stringent than those in this Agreement.

5.2 **Compelled Disclosure**. If a Receiving Party is compelled by law to disclose Confidential Information of the Disclosing Party, it shall provide Disclosing Party with prior notice of such compelled disclosure to the extent legally permitted and reasonable assistance, at Disclosing Party's cost, if Disclosing Party wishes to contest the disclosure.

5.3 **Right to Seek Injunction**. If a Receiving Party discloses or uses (or threatens to disclose or use) any Confidential Information of Disclosing Party in breach of confidentiality protections hereunder, Disclosing Party shall have the right, in addition to any other remedies available to it, to seek

injunctive relief to enjoin such acts, it being specifically acknowledged by the Parties that any other available remedies are inadequate.

6. INTELLECTUAL PROPERTY

6.1 **Proprietary Rights**. As between Customer and Riskonnect, Riskonnect (and the Licensors, where applicable) is the exclusive owner of all right, title and interest, including all related Intellectual Property Rights, in and to the Riskonnect Service, including without limitation any modifications, updates, revisions or enhancements thereto and any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Customer or Users, and regardless of any participation or collaboration by Customer in the design, development or implementation of the Riskonnect Service. No title or ownership of Intellectual Property Rights in and to the Riskonnect Service, or any component thereof, is transferred to Customer, its Affiliates or any third parties hereunder. To the extent that any such Intellectual Property Rights do not otherwise vest in Riskonnect or its Licensors, Customer hereby assigns such Intellectual Property Rights to Riskonnect or its Licensors and agrees to take steps reasonably necessary to perfect Riskonnect's or its Licensors' ownership thereof, without additional consideration of any kind.

6.2 **Proprietary Notices**. Customer shall not remove any copyright, patent, trademark or other proprietary or restrictive notice or legend contained in the Riskonnect Service, and Customer shall reproduce all such notices and legends on all copies of the Riskonnect Service that are permitted to be made hereunder. Customer further agrees to reasonably cooperate with and assist Riskonnect (at Riskonnect's sole expense) in protecting, enforcing and defending Riskonnect's rights in and to the Riskonnect Service.

7. FEES AND PAYMENTS

7.1 **Fees**. Customer shall pay to Riskonnect the fees as set forth in the applicable Subscription Order or Statement of Work or as otherwise agreed in writing by the Parties. Fees for additional services or expenses, if any, will be invoiced monthly as incurred.

7.2 **Expenses**. Customer shall reimburse Riskonnect for all reasonable, documented out of pocket travel, lodging, meal and other expenses incurred by Riskonnect while performing Professional Services. Riskonnect will comply with all reasonable Customer travel and expense policies provided to Riskonnect.

7.3 **Taxes**. Customer shall be liable for any taxes (including but not limited to federal manufacturers' and retailers' excise, state and local sales and use taxes, value added taxes, and personal property taxes), public charges, tariffs, and export and import duties, however designated, and any interest and penalties thereon, arising under this Agreement, other than taxes based on Riskonnect's income. Any taxes assessable on Customer's use of the Riskonnect Service shall also be borne by Customer. All such taxes shall be included in amounts invoiced to Customer.

7.4 **Payments**. All undisputed fees under this Agreement shall be payable by Customer pursuant to and in accordance with any payment schedule set forth in the applicable Subscription Order or Statement of Work or as otherwise agreed by the Parties and shall be due within 30 days of invoice date. Invoices shall be issued by Riskonnect or its Affiliates, as appropriate. All invoices are deemed final unless Customer notifies Riskonnect at billing@riskonnect.com of a dispute in writing within 30 days after receipt of the invoice.

7.5 **Late Payment**. Payments remitted after 15 days after due date on any undisputed portion of an invoice shall bear interest at 1% per month or, if less, the maximum rate allowed by law. If Customer does not pay an invoice 60 days after its due date, Riskonnect may at its sole discretion suspend

Customer's services or terminate this Agreement. Upon termination for non-payment, this Agreement and all of Customer's rights hereunder will terminate without further notice.

7.6 **Fees Generally**. Except as otherwise agreed in writing, Customer acknowledges and agrees that:

7.6.1 fees are set forth in a Subscription Order or Statement of Work;

7.6.2 except as set forth in Sections 12.3.4 and 8.5.2, all payment obligations are non-cancellable, and all fees paid are non-refundable;

7.6.3 all fees shall be paid in _____; and

7.6.4 subject to applicable Data Protection Laws and Regulations, Riskonnect reserves the right to refuse to perform any Professional Services, including but not limited to extraction of Customer Data, should the Customer have any unpaid invoices.

7.7 **Fee Changes**. Riskonnect reserves the right to modify its fees and charges on any anniversary of the Effective Date, as set forth in a Subscription Order.

7.8 **Customer Billing Obligations**. Customer shall provide Riskonnect with complete and accurate billing and billing contact information, including Customer's legal name, street address, name and telephone number and-email address of an authorized billing contact, and any applicable tax exemption certificate number. Customer shall update this information within 30 days of any change by emailing billing@riskonnect.com.

8. TERM AND TERMINATION.

8.1 **Term of the Agreement**. The Term shall commence upon the Effective Date and continue until (i) all Subscriptions hereunder have expired or been terminated, or (ii) the Agreement has been terminated in accordance with this Section 8.

8.2 **Subscription Term**; **Automatic Renewal of Subscriptions; Price Adjustments**. Except as otherwise specified in a Subscription Order, subscriptions will automatically renew for additional periods equal to the expiring subscription term (each, a "**Renewal Subscription Term**") unless one Party notifies the other Party in writing of such Party's election to not renew no later than 90 days prior to the expiration of the Initial Subscription Term or applicable Renewal Subscription Term. Riskonnect will notify Customer of pricing for the Renewal Subscription Term no later than 120 days prior to the date of expiration. Unless one Party notifies the other Party of its election not to renew as provided in this Section, then at least 30 days before the applicable anniversary of the Effective Date, Riskonnect will issue Customer an invoice for fees due for any Renewal Subscription Term, and Customer agrees to pay such invoice in accordance with Section 7.4. The Initial Subscription Term and any Renewal Subscription Term are, collectively, the "Subscription Term."

8.3 **Termination for Cause**. Unless otherwise specified herein, either Party has the right to terminate this Agreement due to a material breach of this Agreement by the other Party if such material breach is not cured within 30 days following receipt of written notice.

8.4 **Termination by Riskonnect for User Breach**. In addition to any other rights granted to Riskonnect herein or under law, Riskonnect reserves the right, upon written notice to Customer, to (i) terminate this Agreement; (ii) terminate subscriptions, in whole or in part; and/or (iii) suspend Customer's access to and use of the Riskonnect Service due to Customer's failure to cause a User to comply with the terms of this Agreement.

8.5 **Effect of Termination**. Upon the expiration or termination of this Agreement for any reason, Customer shall (i) promptly cease all use of the Riskonnect Service; (ii) promptly discontinue

providing access to Users and remove all links to the Riskonnect Service; (iii) within 10 business days after expiration or earlier termination of this Agreement (a) return to Riskonnect, or (b) upon Riskonnect's request, destroy, all copies of the Riskonnect Service in Customer's and the Users' possession or control; and, (iv) within 15 business days after expiration or earlier termination of this Agreement, certify in writing to Riskonnect that it has done all of the foregoing. Customer Data shall be returned and/or disposed of in accordance with the terms and conditions of the applicable Product Schedule.

8.5.1 Upon any expiration or termination of this Agreement,(a) Riskonnect shall invoice Customer for all accrued fees, including, without limitation, the full amount of any implementation fees specified in any applicable Statements of Work, and all reimbursable expenses, and Customer shall pay the invoiced amounts, including from previously issued invoices, within 10 business days of Customer's receipt of such invoice or, if applicable, of the expiration or earlier termination of this Agreement; and (b) Riskonnect shall destroy and/or return, at Customer's request, Customer Data in Riskonnect's standard product format and layout (such destruction or return may be more fully described in a Product Schedule or Security Exhibit), subject to use of any Annual Service hours or execution of a Statement of Work if applicable.

8.5.2 Unless otherwise agreed in a Statement of Work, should Customer terminate this Agreement for Riskonnect's uncured material breach under Section 8.3, Riskonnect shall refund Customer any pre-paid, pro-rated fees to the extent Riskonnect receives a refund from the applicable Licensor.

9. PROFESSIONAL SERVICES

9.1 Professional Services. During the Term, Riskonnect shall perform the Professional Services set forth in the applicable Statement(s) of Work in accordance with the terms of this Agreement.

10. SUPPORT

10.1 Support. Riskonnect shall provide the following support services to Customer:

10.1.1 Software Support in accordance with the Service Level Agreement; and

10.1.2 Annual Services for the number of hours per year, if purchased and included in an applicable Subscription Order. If Customer exceeds the number of Annual Services hours in a given year, then Riskonnect shall notify Customer and upon written agreement for the purchase of more Annual Services hours, invoice Customer for those additional hours used at Riskonnect's then current hourly rate for such Annual Services hours, and Customer agrees to pay in accordance with this Agreement. All Annual Services hours must be used within the twelve months of grant and may not be carried over to any subsequent twelve-month periods.

10.2 Limitations. Riskonnect will not provide any support required as a result of, or with respect to, Customer's operating systems, networks, hardware, or other related equipment, or for Customer's or any of its Users' use of the Riskonnect Service other than in accordance with the applicable Statement of Work and Documentation or as otherwise permitted under this Agreement.

11. LIMITED WARRANTIES AND DISCLAIMER.

11.1 Application Warranty. Riskonnect warrants that a Riskonnect Application will perform in all material respects in accordance with the Documentation when used in accordance with the terms of this Agreement.

11.2 Application Warranty Remedy. Customer's sole remedy for any breach by Riskonnect of the warranty provided in Section 11.1 shall be repair or replacement of the nonconforming functionality in the Riskonnect Application caused by Riskonnect, at Riskonnect's sole expense, as described herein. If Customer discovers that any functionality in the Riskonnect Application fails to conform to the warranty provided in Section 11.1, Customer shall give Riskonnect written notice of such nonconformity no later than 30 days after delivery of the Riskonnect Application or component thereof to Customer.

11.3 Professional Services Warranty. Riskonnect warrants that the Professional Services shall be performed by personnel in a workmanlike manner consistent with the standard of care exercised within the industry.

11.4 Virus Warranty. Riskonnect warrants that, to the best of Riskonnect's knowledge, prior to its access by Customer, the Riskonnect Application does not contain any Disabling Code. Riskonnect will apply commercially reasonable practices and security procedures to avoid insertion of Disabling Code into the Riskonnect Application and, as Customer's sole remedy, Riskonnect shall remove any such Disabling Code so inserted at Riskonnect's cost and expense should Customer not be in breach of its warranty under Section 11.6.

11.5 RISKONNECT WARRANTY DISCLAIMERS.

11.5.1 EXCEPT AS OTHERWISE EXPRESSLY STATED IN THIS AGREEMENT, NEITHER RISKONNECT NOR ITS LICENSORS MAKE ANY WARRANTY OR REPRESENTATION WHATSOEVER, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO THE RISKONNECT SERVICE OR ANY PROFESSIONAL SERVICES PROVIDED UNDER THIS AGREEMENT, INCLUDING QUALITY, PERFORMANCE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. NO RISKONNECT AGENT OR EMPLOYEE IS AUTHORIZED TO MAKE ANY EXPANSION, MODIFICATION OR ADDITION TO THIS LIMITATION AND EXCLUSION OF WARRANTIES IN THIS AGREEMENT.

11.5.2 Customer agrees and acknowledges that Riskonnect and its Affiliates shall not be responsible for any acts, omissions, delays, inaccuracies, errors or any other failure caused by Customer, its Affiliates or any Users' computer systems, hardware or software, including through interfaces with third-party software, or any inaccuracies that such systems may cause within the Riskonnect Service; any inaccuracies in or failures of a Riskonnect Application to conform to the Documentation arising out of the use of a version or release of a Riskonnect Application other than the most recent version or release provided by Riskonnect; any data that Riskonnect receives from Customer or third-party sources, including the data's accuracy or completeness; Customer's claim handling decisions; Customer's failure to encrypt Customer Data; Customer's failure to use available security features within the Riskonnect Service; or, the Riskonnect Service to the extent it is modified by anyone other than Riskonnect.

11.5.3 To the extent the Riskonnect Service uses Internet systems to transmit data or communications, Riskonnect disclaims any liability for interception of any such data or communications, including of encrypted data not solely due to Riskonnect's breach of its obligations hereunder.

11.5.4 Customer agrees that Riskonnect shall have no responsibility or liability for any costs, claims, liabilities, damages or expenses arising in connection with access to or use of the Riskonnect Service by Customer, its Affiliates, or Users other than as authorized by this Agreement.

11.5.5 Customer acknowledges that Riskonnect is also not responsible for and shall have no liability to the Customer, except as expressly set forth in this Agreement, for the security, reliability or continued availability of the telephone lines and equipment outside of Riskonnect's direct control used to access a Riskonnect Service.

11.6 Customer's Warranties. Customer warrants that:

11.6.1 Customer owns all right, title, and interest in and to, or otherwise has the right to grant the use of Customer Data and associated Intellectual Property Rights as set forth in this Agreement;

11.6.2 Customer, and such other third parties used by Customer, are authorized to collect, use and disclose the Customer Data to Riskonnect for use and storage pursuant to this Agreement;

11.6.3 such disclosure, use or storage does not and shall not violate applicable law or, if applicable, any Customer agreements with, or privacy notices to, individuals with respect to whom the Customer Data relates; and

11.6.4 Customer shall use commercially reasonable practices to avoid insertion of Disabling Code into Customer Data or the Riskonnect Service.

12. INDEMNIFICATION

12.1 Riskonnect's Indemnification Obligations. Subject to Section 12.5 below, Riskonnect shall defend, indemnify, and hold Customer, its officers, directors and employees harmless from and against any and all claims, costs, damages, losses, liabilities and expenses (including reasonable attorneys' fees and costs) arising out of or in connection with a third-party claim alleging that the Riskonnect Application infringes or misappropriates the Intellectual Property Rights of a third party.

12.2 Exceptions from Indemnification. Riskonnect's indemnification obligations under Section 12.1 shall not apply where the claim is based in whole or in part on: modifications to a Riskonnect Application or any component thereof made by anyone other than Riskonnect; use of a Riskonnect Application in combination with a product not supplied by Riskonnect; use of a Riskonnect Application other than in accordance with this Agreement or the Documentation; use of a version of a Riskonnect Application other than the most recent version or release provided to Customer by Riskonnect; or errors and omissions caused by third parties that Customer uses to transmit data to or from Riskonnect.

12.3 Riskonnect's Mitigation Obligations. If a Riskonnect Application or any part of a Riskonnect Application is held to infringe the Intellectual Property Rights of a third party and the use thereof is enjoined or restrained or, if as a result of a settlement or compromise, such use is materially adversely restricted, Riskonnect shall, at its own expense and as Customer's sole remedy therefor, either:

12.3.1 procure for Customer the right to continue to use the Riskonnect Application; or

12.3.2 modify the Riskonnect Application to make it non-infringing, provided that such modification does not materially adversely affect Customer's authorized use of the Riskonnect Application; or

12.3.3 replace the Riskonnect Application with a functionally equivalent non-infringing application at no additional charge to Customer; or

12.3.4 if none of the foregoing alternatives is reasonably available to Riskonnect, terminate this Agreement and refund to Customer any prepaid but unearned Fees paid to Riskonnect in advance by Customer prior to the effective date of the termination.

12.4 Customer's Indemnification Obligations. Subject to Section 12.5 below, Customer shall defend, indemnify, and hold Riskonnect, its Licensors and each such Party's parent organizations, subsidiaries, Affiliates, officers, directors and employees harmless from and against any and all claims, costs, damages, losses, liabilities and expenses (including reasonable attorneys' fees and costs) arising out of or in connection with a third-party claim alleging that:

12.4.1 use of Customer Data infringes the rights of, or otherwise harms, a third party; or

12.4.2 Customer's access to or use of the Riskonnect Service, Confidential Information or Intellectual Property Rights of Riskonnect or its Licensors is in violation of this Agreement.

12.5 Procedure. As an express condition of the foregoing indemnification obligations, the Parties hereby agree that:

12.5.1 the indemnified Party shall promptly (and in no event more than 7 days after receipt or discovery) notify the indemnifying Party in writing, of any threat, warning, or notice of any such claim or action, with copies of all documents which the Indemnified Party may receive relating thereto;

12.5.2 the indemnified Party shall cooperate with all reasonable requests of the indemnifying Party (at the indemnifying Party's expense) in defending or settling such claim;

12.5.3 the indemnifying Party shall be allowed to control the defense and settlement of such claim;

12.5.4 the indemnified Party shall have the right, at its option and expense, to participate in the defense of any action, suit or proceeding relating to such a claim through counsel of its own choosing;

12.5.5 the indemnifying Party may not settle any claim that includes an admission of liability, fault, negligence or wrongdoing on the part of the indemnified Party unless the indemnified Party provides prior written consent, or unless the indemnifying Party and the third party unconditionally releases the indemnified Party of all liability that is the subject of the indemnification obligation and such settlement does not adversely affect the indemnified Party's business; and

12.5.6 each indemnified Party will undertake commercially reasonable efforts to mitigate any loss or liability resulting from an indemnification claim related to or arising out of this Agreement.

13. LIMITATIONS OF LIABILITY

13.1 No Consequential Damages. IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY OR ANY THIRD PARTY FOR ANY LOST PROFITS, REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

13.2 Maximum Aggregate Liability. IN RECOGNITION OF THE RELATIVE RISKS AND BENEFITS OF THIS AGREEMENT TO BOTH PARTIES, THE RISKS HAVE BEEN ALLOCATED BY THE PARTIES, AND THE PARTIES AGREE, TO THE FULLEST EXTENT PERMITTED BY LAW, THAT IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF THIS AGREEMENT EXCEED THE AMOUNTS

ACTUALLY PAID OR PAYABLE BY CUSTOMER UNDER THIS AGREEMENT IN THE 12-MONTH PERIOD IMMEDIATELY PRECEDING THE DATE ON WHICH SUCH CLAIM IS MADE AGAINST THE APPLICABLE PARTY.

13.3 No Liability of Riskonnect's Licensors. IN NO EVENT SHALL RISKONNECT'S LICENSORS HAVE ANY LIABILITY TO CUSTOMER OR ANY USER FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR DAMAGES BASED ON LOST PROFITS, HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT CUSTOMER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

13.4 Exemptions from Limitations. NOTHING IN THIS AGREEMENT SHALL EXCLUDE OR LIMIT EITHER PARTY'S LIABILITY FOR (A) DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE; (B) FRAUD OR FRAUDULENT MISREPRESENTATION; (C) ANY LIABILITY THAT CANNOT BE LIMITED OR EXCLUDED BY APPLICABLE LAW

14. GENERAL

14.1 Assignment. Neither Party may assign any of its rights or obligations under this Agreement, whether by operation of law or otherwise, without the other Party's prior written approval (not to be unreasonably withheld); provided, however, either Party may assign this Agreement in its entirety without the other Party's consent to (i) an Affiliate or (ii) in connection with a merger, acquisition, corporate reorganization, change in control, or sale of all or substantially all of its assets. Subject to the foregoing, this Agreement will bind and inure to the benefit of the Parties, their respective successors and permitted assigns. Any purported assignment in violation of this Section 14.1 shall be void.

14.2 Promotional Use. Riskonnect may publicize the fact that Customer has engaged in the authorized use of the Riskonnect Service. Riskonnect may also use Customer's name and brand image or trademark according to Customer's published guidelines for such use and will not state or imply that Customer endorses or recommends the Riskonnect Service.

14.3 Aggregated and De-Identified Information. Riskonnect or its Affiliates may collect and process information about Customer's use of the Riskonnect Service, may analyze and aggregate such data and information with data and/or information Riskonnect may have obtained or may in the future obtain from other of its customers, publicly available sources and/or data providers, and may disclose such analyses and aggregated data to individual prospective or current customers, provided that (i) such data is aggregated and de-identified prior to such use, (ii) Riskonnect does not use such aggregated and de-identified data in a manner which would allow identification of Customer or individuals, and (iii) Customer Data is not transferred to such prospective or current customers. Subject to Riskonnect's confidentiality obligations set forth in Section 5 herein, Customer agrees that Riskonnect or its Affiliates may use aggregated and de-identified data for these purposes.

14.4 Reporting. If Customer licenses a Riskonnect Application that contains reporting functionality (as further described in an applicable Subscription Order), Customer agrees to comply with the terms set forth in **Schedule C**.

14.5 Construction and Interpretation. This Agreement may be executed and delivered by original signature or any image capturing technology (including by electronic signature), and in one or more counterparts, each of which will be deemed to be an original copy of this Agreement and all of which, when taken together, will be deemed to constitute one and the same document. The Section

and paragraph headings contained herein are for convenience of reference only and shall not be considered as substantive parts of this Agreement. The use of the singular or plural form shall include the other form and the use of the masculine, feminine or neuter gender shall include the other genders. In construing or interpreting this Agreement, the word "including" shall not be limiting and the word "hereunder" shall mean under this Agreement. The Parties agree that this Agreement shall be fairly interpreted in accordance with its terms without any strict construction in favor of or against either Party and that ambiguities shall not be interpreted against the drafting Party. In the event of a conflict between a SOW and these Terms and Conditions, the SOW shall govern, but only with respect to the Professional Services set forth in such SOW. In the event of a conflict between these Terms and Conditions and the Supplemental Materials, these Terms and Conditions shall govern. In the event of a conflict between the Agreement and a Customer's code of conduct, the terms of this Agreement shall govern.

14.6 Entire Agreement. This Agreement comprises the entire agreement between Customer and Riskonnect and supersedes all prior or contemporaneous negotiations, discussions or agreements, whether written or oral, between the Parties regarding the subject matter contained herein. For avoidance of doubt, any non-disclosure agreement previously executed between the Customer and Riskonnect is hereby terminated. No text, terms or conditions set forth on any other purchase order, preprinted form or other electronic or non-electronic document not expressly incorporated into this Agreement shall add to or vary the terms and conditions of this Agreement unless otherwise signed by authorized representatives of the Parties. Riskonnect shall not be required to sign a purchase order. Without limiting the generality of the foregoing, no provisions of any shrink-wrap, click-through, online terms or other form of agreement that may be made available by Customer or otherwise exchanged between the Parties constitute a binding agreement or serve to modify the provisions of this Agreement, even if a user or authorized representative of Riskonnect purports to have affirmatively accepted those provisions. Riskonnect shall not be required to enter into any agreement with a third-party data provider regarding data interfaces or the provision of Customer Data under this Agreement.

14.7 Notice.

14.7.1 Any notice or other communication given by a Party under this Agreement shall:

14.7.1.1 be in writing and in English;

14.7.1.2 be signed by, or on behalf of, the Party giving it (except for notices sent by e-mail); and

14.7.1.3 be sent to the relevant Party at the address set out in Section 14.8.3.

14.7.2 Notices may be given, and are deemed received:

14.7.2.1 by hand: on receipt of a signature at the time of delivery;

14.7.2.2 Royal Mail Recorded Signed For post: at 9.00 am on the second Business Day after posting;

14.7.2.3 Royal Mail International Tracked & Signed OR Royal Mail International Signed post: at 9.00 am on the fourth Business Day after posting; and

14.7.2.4 by email on receipt of a delivery email from the correct address.

14.7.3 Notices and other communications shall be sent to:

Riskonnect, Inc. for the attention of the CFO:

380 Interstate North Parkway SE, Suite 400
legal@riskonnect.com

and

[insert name of Customer] for the attention of [insert name and/or position]] at:
[insert address]
[insert email address]

14.7.4 Any change to the contact details of a Party as set out in Section 14.8.3 shall be notified to the other Party in accordance with Section 14.8.2 and shall be effective on the date specified in the notice as being the date of such change, or if no date is so specified, 5 Business Days after the notice is deemed to be received.

14.7.5 All references to time are to the local time at the place of deemed receipt.

14.7.6 This Section does not apply to notices given in legal proceedings or arbitration.

14.7.7 A notice given under this Agreement is not validly served if sent by e-mail only.

14.8 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, then such provision(s) shall be construed, as nearly as possible, to reflect the intentions of the invalid or unenforceable provision(s), with all other provisions remaining in full force and effect.

14.9 Relationship of the Parties. No joint venture, partnership, employment, or agency relationship exists between Customer and Riskonnect as a result of this Agreement or use of the Riskonnect Service.

14.10 Third-Party Beneficiaries. Except as may be provided in the applicable Product Schedule, there are no third-party beneficiaries to this Agreement.

14.11 No Waiver of Rights. The failure of either Party to enforce any right or provision in this Agreement shall not constitute a waiver of such right or provision unless acknowledged and agreed to by either Party in writing.

14.12 Export Control. Riskonnect and Customer shall comply with the export laws and regulations of the United States and other applicable jurisdictions in providing and using the Riskonnect Service and Professional Services. Without limiting the foregoing, each Party represents that it is not named on any U.S. government denied party or sanctioned list. Customer hereby represents and warrants that it shall not permit Users to access or use the Riskonnect Service in a U.S.-embargoed country or in violation of any U.S. export law or regulation and shall indemnify Riskonnect and its employees, officers, directors, and agents from any breach of this warranty.

14.13 Force Majeure. Neither Party shall be liable to the other for any failure or delay in the performance of its obligations (except for required payment obligations above) for any cause that is beyond the reasonable control of such Party, including, without limitation, acts of God, shortages of supplies, labor or materials, strikes and other labor disputes, storms, floods, acts of war or terrorism, failure of third-party hardware, software, services or networks, failure of service providers, utility blackouts or brownouts, failure of telecommunications or the internet, and actions by a governmental authority (such as changes in government codes, ordinances, laws, rules, regulations, or restrictions).

14.14 Surviving Provisions. Except as otherwise set forth herein, in the event of termination of this Agreement for any reason, the provisions of Sections 1, 2.4, 3.4, 4, 5, 6, 8.5.2, 11.5, 11.6, 13, and 14 (except 14.1 and 14.2), as well as all payment obligations, shall survive such termination.

14.15 Governing Law. This Agreement shall be governed in accordance with the laws of England and Wales, without regard to any conflicts of law provision thereof. The United Nations Convention on Contracts for the International Sale of Goods is specifically excluded from application to this Agreement.

14.16 Disputes; Mediation; Binding Arbitration; Emergency Relief.

14.16.1 All claims and disputes between the Parties arising under or relating to this Agreement shall first be presented for mediation by a Party providing written notice to the other Party of its intent to mediate.

14.16.2 If that mediation does not resolve the dispute within forty-five (45) business days of said notice, all claims and disputes arising under or relating to this Agreement are to be settled by binding arbitration under Rules of Arbitration of the International Chamber of Commerce ("**ICC Rules**") in London, UK unless another location is mutually agreeable to the Parties. The arbitration shall be conducted in the English language on a confidential basis pursuant to the ICC Rules.

14.16.3 Any decision or award as a result of any such arbitration proceeding shall be in writing and shall provide an explanation for all conclusions of law and fact and shall include the assessment of costs, expenses, and reasonable attorneys' fees. Any such arbitration shall be conducted by an arbitrator experienced in cloud-based web services and shall include a written record of the arbitration hearing. The Parties reserve the right to object to any individual employed by or affiliated with a competing organization or entity. Judgment upon the award of arbitration may be entered in any court of competent jurisdiction.

14.17 Compliance with Anti-Bribery Laws. Each Party acknowledges that it is aware of, understands and has complied and will comply with, all applicable U.S. and foreign anti-corruption laws, including without limitation, the U.S. Foreign Corrupt Practices Act of 1977 and the U.K. Bribery Act of 2010, and similarly applicable anti-corruption and anti-bribery laws ("**Anti-Corruption Laws**"). Each Party agrees that no one acting on its behalf will give, offer, agree or promise to give, or authorize the giving directly or indirectly, of any money or other thing of value, including travel, entertainment, or gifts, to anyone as an unlawful inducement or reward for favorable action or forbearance from action or the exercise of unlawful influence (a) to any governmental official or employee (including employees of government-owned and government-controlled corporations or agencies or public international organizations), (b) to any political party, official of a political party, or candidate, (c) to an intermediary for payment to any of the foregoing, or (d) to any other person or entity in a corrupt or improper effort to obtain or retain business or any commercial advantage, such as receiving a permit or license, or directing business to any person. Improper payments, provisions, bribes, kickbacks, influence payments, or other unlawful provisions to any person are prohibited under this Agreement.

SCHEDULE A
PRODUCT SCHEDULE

SUPPLEMENTAL TERMS AND CONDITIONS (ACTIVE RISK APPLICATIONS)

The following additional and amended definitions, additional terms and conditions and additional documents are incorporated into the Agreement by reference to the extent Customer has subscribed to one of the following Active Risk applications (collectively, "**Active Risk Applications**") offered via the Platform Service described below as more fully set forth on a Subscription Order and/or SOW:

- Active Risk Manager (ARM)
- Active Risk Compliance Manager (ARCM)
- Active Risk Operational Risk Manager (ARORM)
- Active Risk Audit Manager (ARAM)
- Active Risk Quality Manager (ARQM)
- Active Risk Policy Manager (ARPM)

For clarity, these Active Risk Applications may also be referred to in this **Schedule A** as the Riskonnect Service. All defined terms in this **Schedule A** have the meanings set forth in the General Terms and Conditions, as and to the extent amended below.

1. Additional and Amended Definitions

1.0 "**Data Infrastructure**" means the data processing resources within the Riskonnect Service, including but not limited to, data and file storage, within Customer's account configured in the Riskonnect Service platform.

1.1 "**Licensors**" means:

1.1.1 Aspose

1.1.2 Exago

1.1.3 Font Awesome

1.1.4 Highcharts

1.1.5 Kendo

1.1.6 SnappIT

1.1.7 Verify

1.2 "**Platform Provider**" means Amazon Web Services or Microsoft Azure.

1.3 "**Platform Service**" means the online, web-based service provided by Platform Provider to Riskonnect in connection with Riskonnect's provision of the Riskonnect Service.

1.4 "**System Administrator**" means a User designated by Customer who is authorized to create User accounts, to purchase subscriptions by executing a Subscription Order, and to otherwise administer Customer's use of the Riskonnect Service.

2. Additional Terms and Conditions

2.0 **Modifications Performed by Customer**. Any configuration, development, or data integration services to Customer's instance of the Riskonnect Service that is performed by Customer or Customer's third parties is not covered by Software Support, and Riskonnect shall have no liability whatsoever for such services. However, Customer may request Riskonnect to render support services for configurations and modifications performed by Customer provided that such Annual Services shall be billable to Customer at Riskonnect's then current hourly rate.

2.1 **Data Infrastructure**. Customer's subscription includes a specific quantity of Data Infrastructure, as set forth on the applicable Subscription Order. The Riskonnect Service includes administrative features that permit Customer's System Administrator(s) to view and monitor Customer's utilization of Data Infrastructure. If Customer exceeds the amount of Data Infrastructure as set forth in the Subscription Order, Customer shall be charged for any additional Data Infrastructure used and pay additional subscription fees. Provided that any such changes do not adversely impact Customer Data Infrastructure limits or rights as agreed to in this Agreement, Riskonnect reserves the right to establish or modify with thirty (30) days' notice its general Data Infrastructure practices and limits, provided the minimum amount of storage included without additional charge may not be modified without Customer's prior written consent.

2.2 **Third-Party Beneficiaries.** There are no third-party beneficiaries of this Agreement, except that the Platform Provider shall be a third-party beneficiary of this Agreement solely as it relates to the disclosure and use of any confidential or proprietary information of the Platform Provider that Riskonnect may disclose to Customer.

3. Service Level Agreement.

3.0 The Service Level Agreement found at https://riskonnect.com/legal-sla/ is incorporated herein by this reference.

SUPPLEMENTAL TERMS AND CONDITIONS (RISKONNECT APPLICATIONS)

The following Additional and Amended Definitions, Additional Terms and Conditions and Additional Exhibits are incorporated into the Agreement by reference to the extent Customer has subscribed to one of the following Riskonnect Applications offered via the Platform Service described below as more fully set forth on a Subscription Order and/or SOW:

- Integrated Risk Management Services (IRMS)
- Risk Management Information System (RMIS)
- Health & Safety (H&S)
- HealthCare
- Enterprise Risk Management
- Internal Audit
- Regulatory & Compliance Management
- Sarbanes Oxley - SOX
- Third Party Risk Management

All defined terms in this Schedule A have the meanings set forth in the General Terms and Conditions, as and to the extent amended below.

1. Additional and Amended Definitions:

1.1 "**Data Infrastructure**" means the data processing resources within the Riskonnect Service, including but not limited to, data and file storage, within Customer's account configured in the Riskonnect Service platform.

1.2 "**Licensors**" shall also include:

1.2.1 salesforce.com (Platform Provider);

1.2.2 Rackspace (secure server environment for converting source data);

1.2.3 Adobe EchoSign (e-signature);

1.2.4 Domo (Riskonnect Insights data visualization); and

1.2.5 Other subprocessors as identified in the Data Processing Addendum.

1.3 "**Platform Provider**" means Salesforce.com, Inc.

1.4 "**Platform Service**" means the online, web-based service provided by Platform Provider to Riskonnect in connection with Riskonnect's provision of the Riskonnect Service.

1.5 "**System Administrator**" means a User designated by Customer who is authorized to create User accounts, to purchase subscriptions by executing a Subscription Order, and to otherwise administer Customer's use of the Riskonnect Service.

2. Additional Terms and Conditions

2.1 **Sole Provider**. Notwithstanding any access Customer's Users may have to the services of Riskonnect's Licensors via the Customer's configuration of the Riskonnect Service, Riskonnect is the sole provider of the Riskonnect Service and Customer is entering into a contractual relationship solely with Riskonnect. In the event that Riskonnect ceases operations or otherwise ceases or fails to provide the Riskonnect Service, Riskonnect's Licensors have no obligation to refund Customer any fees paid by Customer to Riskonnect or to provide Customer the Riskonnect Service.

2.2 **Modifications Performed by Customer**. Any configuration, development, or data integration services to the Customer's instance of the Riskonnect Service that is performed by Customer or Customer's third parties is not covered by Software Support and Riskonnect shall have no liability whatsoever for such services. However, Customer may request Riskonnect to render support services for configurations and modifications performed by Customer provided that such Annual Services shall be billable to Customer at Riskonnect's then current hourly rate.

2.3 **Data Infrastructure**. Customer's subscription includes a specific quantity of Data Infrastructure, as set forth on the applicable Subscription Order. The Riskonnect Service includes administrative features that permit Customer's System Administrator(s) to view and monitor Customer's utilization of Data Infrastructure. If Customer exceeds the amount of Data Infrastructure as set forth in the Subscription Order, Customer shall be charged for any additional Data Infrastructure used and pay additional subscription fees. Provided that any such changes do not adversely impact Customer Data Infrastructure limits or rights as agreed to in this Agreement, Riskonnect reserves the right to establish or modify with thirty (30) days' notice its general Data Infrastructure practices and limits, provided the minimum amount of storage included without additional charge may not be modified without Customer's prior written consent.

2.4 **Licensors' Warranty Disclaimer**. NOTHING IN THIS SCHEDULE A, SECTION 2.4 SHALL LIMIT RISKONNECT'S WARRANTIES OR INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT, INCLUDING THOSE THAT RISKONNECT MAKES AND/OR PROVIDES ON BEHALF OF RISKONNECT'S LICENSORS. Notwithstanding the foregoing, to the maximum extent permitted by law, Riskonnect's Licensors make no, and disclaim all, warranties of any kind, whether express, implied, statutory, or otherwise, including, without limitation, any implied warranty of merchantability, fitness for a particular purpose, or non-infringement of third-party rights with respect to the Platform Service, and/or the Riskonnect Service, or any of the products and services offered by Riskonnect's Licensors. Riskonnect's Licensors make no representation, warranty, or guaranty as to the reliability, timeliness, quality, suitability, availability, accuracy or completeness of the Riskonnect Service. Riskonnect's Licensors do not represent or warrant that the Riskonnect Service will be available, secure, timely, uninterrupted or error-free; the Riskonnect Service or any of the products and services offered by Riskonnect's Licensors will meet Customer's requirements or expectations; any data stored using the Riskonnect Service will be accurate, reliable, or secure; errors or defects in the Riskonnect Service will be corrected; or the Riskonnect Service or the Data Infrastructure used by Riskonnect to make the Riskonnect Service available are free of Disabling Code, viruses or other harmful components.

2.5 **Third-Party Beneficiaries**. There are no third-party beneficiaries to this Agreement, except Platform Provider shall be a third-party beneficiary to this Agreement solely as it relates to the provisions herein that relate to the use of the Platform Service.

2.6 **Data Portability and Deletion**

2.6.1 **Prior to Termination or Expiration**. At any time during the Term of this Agreement, Customer will have access to and the ability to extract the Customer Data. Customer may schedule a weekly data export from within the Riskonnect Service for Customer's own backup purposes.

2.6.2 **After Termination or Expiration**. If this Agreement terminates for any reason, within 30 days of Customer's written request (provided that Riskonnect receives the request before the effective date of termination), Riskonnect will provide Customer Data to Customer in Riskonnect's then current standard format and layout using Customer's

available Annual Service hours or at additional cost, if Customer's Annual Service hours have been exhausted. Riskonnect shall thereafter delete Customer Data. Riskonnect's Data Transfer Protocols shall apply to any transfer of Customer Data under this section.

2.7 **User Access**. It is Customer's responsibility to designate the applicable access to be granted to each User. Customer assumes full legal and financial responsibility for all instructions of any nature that are reasonably accepted and acted upon by Riskonnect in accordance with such designation. Customer shall promptly notify Riskonnect if it becomes aware that the security of its designations has been compromised. Users shall only access, use, and/or configure those modules and features associated with the applicable Riskonnect Application(s) to which Customer subscribes under this Agreement. If a User accesses, uses, configures, and/or replicates a Riskonnect Application module or feature within the Riskonnect Service other than those to which Customer has subscribed, then Riskonnect shall notify Customer of the unauthorized access or use. If such unauthorized access or use by the User is not discontinued within 10 days, then Riskonnect will adjust Customer's subscriptions and invoice Customer for the additional Riskonnect Application, module or feature being accessed or used.

3. Additional Exhibits

The following Exhibits are incorporated into this Schedule A:

Exhibit 1 to Schedule A – Riskonnect Products Special Terms of Use

The Service Level Agreement found at https://riskonnect.com/legal-sla/.

Exhibit 1 to Schedule A

Riskonnect Products Special Terms of Use

A. Riskonnect Insights Terms of Use

Subject to the terms and conditions of the Agreement and this Exhibit 1 (herein "**Exhibit**"), Riskonnect provides Customer's Users a subscription to use Insights expressly for risk-related data.

B. Riskonnect eSignature Terms of Use

4. Subject to the terms and conditions of the Agreement and this Exhibit, Riskonnect provides Customer's Users a subscription to use Riskonnect eSignature which is based upon the Adobe Sign service, formerly Adobe EchoSign Service ("Adobe Sign") in Customer's configuration of the Riskonnect Service for up to two-thousand transactions annually. As a condition of the subscription to Adobe Sign, Customer shall abide by the Adobe Sign terms of use ("**TOU**") located at http://www.adobe.com/legal/terms.html. Riskonnect agrees to notify Customer of any changes to the TOU that have any material negative impact on Customer relative to Customer's configuration of the Riskonnect Service as provided under the Agreement. Except for the express limited rights granted under the Agreement, this Exhibit, and the TOU, no right, title or interest in or to any of Adobe intellectual property or products is granted, transferred or otherwise provided.

5. By using the electronic signature feature of Adobe Sign, Customer agrees to conduct a particular business transaction with electronic documents and electronic signatures instead of paper-based documents and wet ink signatures. Customer is under no obligation to transact business electronically using Adobe Sign.

6. As Riskonnect does not have the capability to verify the identity or the authority of an electronic signatory to a document submitted through Adobe Sign, Customer agrees that Customer is solely responsible for verifying the identity of each other signatory to a document. Riskonnect does not certify the validity, completeness, or enforceability of any document submitted through Adobe Sign.

7. While Adobe Sign complies with the United States Electronic Signatures in Global and National Commerce Act ("**ESIGN**"), Customer shall be solely responsible for compliance as well as its advice, counsel and recommendations of all laws and regulations concerning Customer's use of Adobe Sign regardless of the type of purpose, industry, or country.

8. Except as otherwise required by a court of law having proper jurisdiction over such matters, Riskonnect has no obligation and no duty to become involved in any dispute between Customer and any third party in connection with Customer's use of ADOBE SIGN. IN THE EVENT RISKONNECT BECOMES INVOLVED IN A DISPUTE (E.G., AS A PARTY OR WITNESS) AS A RESULT OF YOUR USE OF ADOBE SIGN, YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS RISKONNECT FROM ANY CLAIM, SUIT OR PROCEEDING BROUGHT AGAINST RISKONNECT BY A THIRD PARTY IN CONNECTION WITH ANY ACTS OR OMISSIONS WITH REGARDS TO YOUR USE OF ADOBE SIGN. The preceding sentence does not apply to disputes concerning the scope of Riskonnect's authority to sublicense Adobe Sign to You, or intellectual property disputes related to or involving Adobe Sign which, like all other disputes, shall be handled in accordance with the Agreement.

9. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THE AGREEMENT AND TOU, ADOBE SIGN IS PROVIDED AS-IS AND RISKONNECT HEREBY DISCLAIMS AND MAKES NO OTHER REPRESENTATION OR WARRANTIES OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY.

10. **Fair Use Policy**. Customer must not use or allow any person to use Adobe Sign in a way that Riskonnect or Adobe reasonably considers to be:

- a breach of any law, code or regulatory standard;
- a breach of the TOU;
- likely to disrupt the provision of services to other Riskonnect customers;
- designed to avoid any restrictions placed by Riskonnect or Adobe on Adobe Sign; or
- otherwise unreasonable or excessive.

If Riskonnect, in its sole discretion, determines that Customer has breached this Fair Use Policy, Riskonnect will notify Customer of the breach and request that the prohibited activity be discontinued. If, after being contacted, Customer continues to be in breach of this Fair Use Policy, Riskonnect may without further notice, limit, suspend or terminate the Customer's Adobe Sign service.

C. Riskonnect Alerts Service Terms of Use

DISCLAIMER OF WARRANTY AND LIABILITY. NOTWITHSTANDING RELATED PROVISIONS IN THE AGREEMENT, RISKONNECT NEITHER MAKES ANY WARRANTY NOR ACCEPTS ANY LIABILITY WITH REGARD TO THE TIMELINESS AND ACCURACY OF THE THIRD-PARTY DATA DELIVERED THROUGH THE RISKONNECT ALERTS SERVICE. FURTHERMORE, THE PARTIES EXPRESSLY AGREE THAT ANY NON-CONFORMITY OR FAILURE OF THE RISKONNECT ALERTS SERVICE SHALL NOT GIVE REASON TO TERMINATE THE AGREEMENT FOR CAUSE.

D. LineSlip Service Additional Terms.

1. License to Use Customer Logos/Trademarks. Customer grants to LineSlip Solutions, Inc. ("**LineSlip**") a license to use Customer's logos/trademarks on Customer's interface of the LineSlip Service or any reports/outputs.

2. Aggregate Data. Both during and after the Term, LineSlip may collect, use, and analyze data provided to LineSlip or otherwise arising during the use of the LineSlip Service, in order to improve and enhance the LineSlip Service and for other development, diagnostic and corrective purposes for those or other offerings of LineSlip, and solely to the extent such data is aggregated or otherwise de-identified in a manner that does not identify Customer, share and commercialize such data.

3. Termination by LineSlip. LineSlip may at any time terminate Customer's access to and use of the LineSlip Service if: (a) LineSlip is required to do so by law (for example, where the provision of the LineSlip Service to Customer is, or becomes, unlawful); (b) in LineSlip's opinion, no longer commercially viable; or (c) LineSlip has elected to discontinue the LineSlip Service (or any part thereof).

4. Third Party Beneficiary. Customer acknowledges and agrees that LineSlip will be a third party beneficiary of the Agreement with respect to the LineSlip Service only.

SUPPLEMENTAL TERMS AND CONDITIONS (RESILIENCE APPLICATIONS)

The following Additional Definitions, Additional Terms and Conditions and Additional Exhibits are incorporated into the Agreement by reference to the extent Customer has subscribed to one or more of the following Riskonnect Applications described below and as more fully set forth on a Subscription Order and/or SOW:

- Resilience Software (including Resilience AI)
- Threat Intelligence Software
- Notifications Software

All capitalized terms used but not otherwise defined in this Schedule A have the meanings set forth in the General Terms and Conditions, except as and to the extent amended below.

1. Additional Definitions:

1.1 "**Communication Platform Provider**" means Twilio (phone, text and email delivery).

1.2 "**Communication Service**" means the online, web-based service provided by Communication Platform Provider to Riskonnect in connection with Riskonnect's provision of the Riskonnect Service.

1.3 "**Customer Contacts**" means Users who access and use the Riskonnect Service to perform plan creation (based on existing templates), update, view and approval.

1.4 "**Internal Contacts**" means those personnel designated by Customer to receive notifications via the Notifications Module.

1.5 "**Licensors**" means, as applicable, depending on Customer's implementation of the Riskonnect Service:

1.5.1 Platform Provider;

1.5.2 DocRaptor (.pdf generation);

1.5.3 Communication Platform Provider; and

1.5.4 SendGrid (subsidiary of Communication Platform Provider used to facilitate email delivery).

1.6 "**Platform Provider**" means Amazon Web Services and/or Microsoft Azure.

1.7 "**Platform Service**" means the online, web-based service provided by Platform Provider (as defined below) to Riskonnect in connection with Riskonnect's provision of the Riskonnect Service.

2. Additional Terms and Conditions.

2.1 As applicable, use of the Notifications Software notification tool is limited to organizational incidents. This includes messages as part of a crisis and ten tests per year (total test messages will not exceed ten times the number of internal contacts within the Riskonnect Service). Additional non-incident-based use may incur additional charges at Riskonnect's sole discretion, up to $0.25 per message sent. Lastly, the Notifications Software is not to be used for internal operational communications among first responders, nor is for use with any third-party customer, supplier, or local population for status update purposes. Customer must only use the Notifications Software for internal communications during an operational disruptive incident or for an exercise to evaluate internal crisis communications-related purposes.

2.2 **Acceptance of Licensor.** Customer hereby accepts and consents to Riskonnect's use of the Communication Platform Provider for the processing of Customer Data.

2.3 **Acceptable Use Policy.** Customer, on behalf of itself and all Users, agrees to comply with Communication Platform Provider's Acceptable Use Policy available at the following web site: https://www.twilio.com/legal/aup (as updated from time to time, "**Use Policy**"). Should Customer or any of its Users materially breach, or should Riskonnect in good faith believe Customer or any of its Users have materially breached, any of the terms of the Use Policy, Riskonnect may suspend the Communication Service upon notice to Customer.

2.4 **Suspension of Communication Services.** Riskonnect may suspend the Communication Service if there is an unusual and material spike or increase in Customer's use of the Communication Service and if Riskonnect suspects that such traffic or use is fraudulent or materially and negatively impacting the operating capability of the Communication Services or if provision of the Communication Service is prohibited by applicable law or regulation.

2.5 **Backwards Compatibility.** If any Updates to the Communication Service that are not backward compatible become necessary, Riskonnect will use commercially reasonable efforts to notify Customer at least thirty (30) days prior to implementation.

2.6 **Feedback and Suggestions.** Customer agrees to assign any intellectual property in feedback and suggestions regarding the Communication Service to the Communication Platform Provider.

2.7 **Communication Platform Provider's Warranty Disclaimer.** NOTHING CONTAINED IN THIS SCHEDULE SHALL LIMIT RISKONNECT'S WARRANTIES OR INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT, INCLUDING THOSE THAT RISKONNECT MAKES AND/OR PROVIDES ON BEHALF OF RISKONNECT'S LICENSORS. NOTWITHSTANDING THE FOREGOING, TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE COMMUNICATION PLATFORM PROVIDER MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, AND SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT TO THE FULLEST EXTENT PERMITTED BY LAW. COMMUNICATION PLATFORM PROVIDER ADDITIONALLY DISCLAIMS ALL WARRANTIES RELATED TO THIRD PARTY TELECOMMUNICATIONS PROVIDERS. CUSTOMER ACKNOWLEDGES THE INTERNET AND TELECOMMUNICATIONS PROVIDERS' NETWORKS ARE INHERENTLY INSECURE AND THAT NEITHER COMMUNICATION PLATFORM PROVIDER NOR RISKONNECT WILL HAVE ANY LIABILITY FOR ANY CHANGES TO, INTERCEPTION OF, OR LOSS OF CUSTOMER DATA WHILE IN TRANSIT VIA THE INTERNET OR A TELECOMMUNICATIONS PROVIDER'S NETWORK.

2.8 **Indemnification.** Customer shall defend Riskonnect, the Communication Platform Provider and the Communication Platform Provider's directors, officers, employees, and Affiliates (collectively, "**Indemnified Parties**") from and against any claim, demand, suit, or proceeding made or brought against an Indemnified Party by a third party alleging or arising out of Customer's breach of the Use Policy. Customer will indemnify the Indemnified Parties from any damages, fines or penalties imposed by a government or regulatory body, attorneys' fees, and costs awarded against an Indemnified Party or for settlement amounts approved by Customer for a claim under this Section. No limitation of liability shall apply to this Section.

2.9 **Third-Party Beneficiaries.** There are no third-party beneficiaries of this Agreement, except that the Platform Provider shall be a third-party beneficiary of this Agreement solely as it relates to the disclosure and use of any confidential or proprietary information of the Platform Provider that Riskonnect may disclose to Customer.

2.10 Resilience AI. Customer acknowledges and agrees that any data that it provides to Riskonnect is subject to Riskonnect's Privacy Notice (https://riskonnect.com/privacy-notice/) and that such data will be shared with OpenAI and will be used by OpenAI in accordance with its then current Privacy Policy (https://openai.com/policies/privacy-policy).

2.11 Data Deletion. Notwithstanding anything to the contrary in the Agreement, Riskonnect shall not have any obligation to return Customer Data to the Customer. No later than thirty (30) days after termination or expiration of the Agreement, Riskonnect shall delete the Customer Data.

2.12 Service Level Agreement. The Service Level Agreement found at https://riskonnect.com/legal-sla/ is incorporated herein by this reference.

OnSolve Products

Customer's access to and use of the products and services licensed to Customer by Riskonnect as an authorized reseller of OnSolve, LLC ("**OnSolve**") under the applicable Order ("**OnSolve Products**") are subject to OnSolve's end user subscription agreement located at https://www.onsolve.com/company/legal/enterprise-terms-and-conditions/ as may be updated from time to time by OnSolve.

In addition, Customer acknowledges and agrees that:

3. OnSolve shall maintain Customer access to and continue to support Customer use of the SendWordNow platform that has been white-labeled and may be referred to as AssuranceNM ("**Legacy Platform**") according to the following schedule:

3.1 End of Maintenance (December 31, 2024). OnSolve shall cease to provide scheduled updates to Legacy Platform after December 31, 2024. OnSolve will continue to provide critical Severity 1 and Severity 2 related break fixes, or security remediations as achievable.

3.2 End of Support (June 30, 2025). OnSolve shall cease to provide any customer support, critical Severity 1 and Severity 2 related break fixes, or security remediations to the Legacy Platform. OnSolve shall have no responsibility for maintaining the Legacy Platform beyond Jund 30, 2025.

3.3 End of Life (December 31, 2025). OnSolve shall terminate the live, operational status of the Legacy Platform for Customer. Customer must be migrated from the Legacy Platform to the OnSolve Products. OnSolve shall have no responsibility for any damages caused to Customer solely to the extent caused by disconnecting, deleting, or otherwise prohibiting its access to the Legacy Platform after December 31, 2025.

Everbridge Solutions

The following terms apply to Customer's access to and use of the Solutions (as defined below):

1. Definitions.

1.1 "**Solutions**" means Everbridge, Inc.'s proprietary interactive communication solutions licensed to Customer under an applicable Order.

1.2 "**Contacts**" are individuals who Customer designates as authorized to receive notifications or other communications through the Solutions and/or who provide their personal contact information to Everbridge, including through an opt-in portal.

1.3 "**Professional Services**" means training and professional services, if any, set forth in the applicable quote.

1.4 "**Services**" means, collectively, the Solutions and the Professional Services.

2. Customer Data. Customer shall maintain a copy of all Contact data it provides to Everbridge.

3. Use of Solutions. Customer shall use the Service in accordance with Everbridge's then applicable Acceptable Use Policy posted on www.everbridge.com. Customer shall promptly notify Everbridge of any unauthorized use of any password or account of which Customer becomes aware. Customer acknowledges that the Solutions are a passive conduit for the transmission of Customer Data, and Everbridge has no obligation to screen, preview or monitor content, and shall have no liability for any errors or omissions or for any defamatory, libelous, offensive or otherwise unlawful content in any Customer Data, or for any losses, damages, claims, or other actions arising out of or in connection with any data sent, accessed, posted or otherwise transmitted via the Solutions by Customer, Users or Contacts, except to the extent such losses are caused directly by the acts or omissions of Everbridge personnel.

4. Proprietary Rights.

4.1 Restrictions. Customer shall use the Solution solely for its internal business purposes. In particular, Customer's use of the Solutions shall not include service bureau use, outsourcing, renting, reselling, sublicensing, or time-sharing. Customer shall not (i) sell, transfer, assign, distribute or otherwise commercially exploit or make the Solution available to any third party except as expressly set forth herein; (ii) modify or make derivative works based upon the Solution; (iii) reverse engineer the Solution; (iv) remove, obscure or alter any proprietary notices or labels on the Solution or any materials made available by Everbridge; (v) use, post, transmit or introduce any device, software or routine (including viruses, worms or other harmful code) which interferes or attempts to interfere with the operation of the Solution; or (vi) defeat or attempt to defeat any security mechanism of any Solution.

4.2 Reservation of Rights. The Solutions (including all associated computer software (whether in source code, object code, or other form), databases, indexing, search, and retrieval methods and routines, HTML, active server pages, intranet pages, and similar materials) and all intellectual property and other rights, title, and interest therein (collectively, "**IP Rights**"), whether conceived by Everbridge alone or in conjunction with others, constitute Confidential Information and the valuable intellectual property, proprietary material, and trade secrets of Everbridge and its licensors and are protected by applicable intellectual property laws of the United States and other countries. Everbridge owns (i) all voluntary feedback regarding the design or operation of the Services (except for the Customer Data) provided to Everbridge by Users, Customer and Contacts in conjunction with the Services, and (ii) all aggregated and anonymized transactional, performance, derivative data and metadata generated in connection with the Solutions, which are generally used to improve the functionality and performance of the Services. Except for the rights expressly granted to Customer in this Agreement, all rights in and to the Solutions and all of the foregoing elements thereof (including the rights to any work product resulting from Professional Services and to any modification, enhancement, configuration or derivative work of the Solutions) are and shall remain solely owned by Everbridge and its respective licensors. Everbridge may use and provide Solutions and Professional Services to others that are similar to those provided to Customer hereunder, and Everbridge may use in engagements with others any knowledge, skills, experience, ideas, concepts, know-how and techniques used or gained in the provision of the Solutions or Professional Services

to Customer, provided that, in each case, no Customer Data or Customer Confidential Information is disclosed thereby.

5. Warranties; Disclaimer.

5.1 Everbridge Warranty and Support Services. Everbridge shall provide the Solutions in material compliance with the functionality and specifications set forth on the applicable Documentation. Everbridge shall provide 24X7X365 customer support in accordance with its most recently published Technical Support Services Guide. Professional Services shall be performed in a professional manner consistent with industry standards.

5.2 Disclaimer. THE FOREGOING REPRESENT THE ONLY WARRANTIES MADE BY EVERBRIDGE HEREUNDER, AND EVERBRIDGE EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. EVERBRIDGE DOES NOT WARRANT THAT THE SOLUTION WILL OPERATE ERROR FREE OR WITHOUT INTERRUPTION. WITHOUT LIMITING THE FOREGOING, IN NO EVENT SHALL EVERBRIDGE HAVE ANY LIABILITY FOR PERSONAL INJURY (INCLUDING DEATH) OR PROPERTY DAMAGE ARISING FROM FAILURE OF THE SOLUTION TO DELIVER AN ELECTRONIC COMMUNICATION, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY, EVEN IF EVERBRIDGE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5.3 SMS Transmission. CUSTOMER ACKNOWLEDGES THAT THE USE OF SHORT MESSAGING SERVICES ("SMS"), ALSO KNOWN AS TEXT MESSAGING, AS A MEANS OF SENDING MESSAGES INVOLVES A REASONABLY LIKELY POSSIBILITY FROM TIME TO TIME OF DELAYED, UNDELIVERED, OR INCOMPLETE MESSAGES AND THAT THE PROCESS OF TRANSMITTING SMS MESSAGES CAN BE UNRELIABLE AND INCLUDE MULTIPLE THIRD PARTIES THAT PARTICIPATE IN THE TRANSMISSION PROCESS, INCLUDING MOBILE NETWORK OPERATORS AND INTERMEDIARY TRANSMISSION COMPANIES. ACCORDINGLY, EVERBRIDGE RECOMMENDS THAT SMS MESSAGING NOT BE USED AS THE SOLE MEANS OF COMMUNICATION IN AN EMERGENCY SITUATION.

6. Indemnification.

6.1 By Everbridge. Everbridge shall defend, indemnify and hold Customer harmless from and against any loss or damage (including reasonable attorneys' fees) incurred in connection with any third-party claim, suit or proceeding against Customer arising out of an allegation that the Solution as provided hereunder infringes an issued patent or other Intellectual Property Rights ("**Claim**"). If (x) any aspect of the Solution is found or, in Everbridge's reasonable opinion is likely to be found, to infringe upon the Intellectual Property Rights of a third party or (y) the continued use of the Solution is enjoined, then Everbridge will promptly and at its own cost and expense at its option: (i) obtain for Customer the right to continue using the Solution; (ii) modify such aspect of the Solution so that it is non-infringing; or (iii) replace such aspect of the Solution with a non-infringing functional equivalent. If, after all commercially reasonable efforts, Everbridge determines in good faith that options (i) - (iii) are not feasible, Everbridge will remove the infringing items from the Solution and refund to Customer on a pro-rata basis any prepaid unused fees paid for such infringing element. The remedies set forth in this Section 9.2 are Customer's exclusive remedy for Claims for infringement of an Intellectual Property Right. Everbridge shall have no obligation or liability for any claim pursuant to this Section to the extent arising from: (i) the combinations, operation, or use of the Solution supplied under this Agreement with any product, device, or software not supplied by Everbridge to the extent the combination creates the infringement; (ii) the unauthorized alteration or modification by Customer of the Solution; or (iii) Everbridge's compliance with

Customer's designs, specifications, requests, or instructions pursuant to an engagement for Everbridge Professional Services relating to the Solution to the extent the claim of infringement is based on the foregoing.

6.2 Indemnification Process. Everbridge's obligations under this Section 6 are contingent upon the Customer: (a) promptly giving Everbridge notice of the Customer once the Claim is known; (b) giving Everbridge sole control of the defense and settlement of the Customer (provided that Everbridge may not settle such Claim unless such settlement unconditionally releases Customer of all liability and does not knowingly adversely affect Customer's business or service); and (c) providing Everbridge all available information and reasonable assistance.

7. Liability Limits. To the maximum extent permitted by law, neither Customer nor Everbridge shall have any liability to the other party for any indirect, special, incidental, punitive, or consequential damages, however caused, under any theory of liability, and whether or not the party has been advised of the possibility of such damage. Except for its indemnification obligations under Section 9.2, notwithstanding anything in this Agreement to the contrary, in no event shall Everbridge's aggregate liability, regardless of whether any action or claim is based on warranty, contract, tort or otherwise, exceed amounts paid or due by Customer to Everbridge hereunder during the 12-month period prior to the event giving rise to such liability. The foregoing limitations shall apply even if the non-breaching party's remedies under this Agreement fail their essential purpose.

8. Additional Business Terms.

The following additional business terms are incorporated by reference into the Agreement as applicable based on the particular products and services described in the Order.

<u>If Customer Is Ordering Nixle® Products or Community Engagement</u>:

8.1 Customer grants to Everbridge a non-exclusive, royalty free, worldwide and perpetual right and license (including sublicense) to (a) use, copy, display, disseminate, publish, translate, reformat and create derivative works from communications Customer sends through the Solutions for public facing communications to citizens, other public groups and public facing websites, including social media (e.g., Google®, Facebook®) (collectively, "**Public Communications**"), (b) use and display Customer's trademarks, service marks and logos, solely as part of the Public Communications to Contacts who have opted in to receive those Communications, and on other websites where Everbridge displays Customer's Public Communications, as applicable, and (c) place a widget on Customer's website in order to drive Contact opt-in registrations. Customer further acknowledges and agrees that all personal information from individuals registering through such widget is owned expressly by Everbridge and such information will be governed by the applicable Privacy Policy.

<u>If Customer Is Ordering Everbridge Suite Products</u>:

8.2 Messaging Credits. The Solutions include units of usage ("**Messaging Credits**") for communications sent by Customer through the Solutions to multiple Contacts via one or more communication paths ("**Notifications**"). No Messaging Credits shall be required to send Notifications by push notification (Everbridge mobile application), by email or by pager. If Customer's use of the Solutions exceeds the amount of Messaging Credits allocated to the account or previously purchased, Customer shall pay for such overages and charges back to the date they were incurred. Unused Messaging Credits expire at the end of the annual billing period under the applicable Order and are not refundable. Additional Messaging Credits may be purchased separately.

8.3 **Usage.** Messaging Credits shall be applied per Notification sent by Customer through the Solutions. A single Notification is defined as follows:

- SMS Text messages:
    - For messages that contain only GSM characters, each 153 characters or portion thereof.
    - For messages that contain any non-GSM characters, each 67 characters or portion thereof.
    - GSM characters include only characters in the GSM 7-bit default alphabet.
    - Character limits for SMS Text messages are determined by telecommunication providers. Everbridge reserves the right to change the length of a single SMS Text message if telecommunication providers update these amounts.
- Voice messages or Conference Voice: One minute or portion of a minute of the voice message, calculated on a cumulative basis per month, per destination country.
- TTY: One minute per TTY message.
- Fax: Per page transmitted.

8.4 **Role-based Limits.** If Customer exceeds any role-based limits (such as the number of Contacts, Resolvers or authorized users of a Solution) set forth on the applicable Order, Customer shall pay for such additional role-based numbers as of the date that the overage began. Payment shall be at the role-based number rate in the Order and shall be paid for the duration of the term of such Order.

8.5 **Other Usage Limits.** If the applicable Order sets forth any geographic, departmental, entity-based, or other limitation on usage of the Solutions, then Customer's use of the Solutions is expressly limited to Contacts who are based in such geographic area, department or entity or who otherwise meet the usage limitation criteria specified in the Order. Customer's use of the Solutions with any Contacts who are not included within such limitations shall constitute a material default under this Agreement and shall subject such Customer to additional charges for such unauthorized usage.

8.6 **Data Feeds.** Customer shall not use any automated device, computer program, software, tool, algorithm, bot or similar process to mine or systematically scrape or extract data from any of the products, except as authorized in writing by Everbridge. Notwithstanding anything to the contrary in this Agreement, to the extent that Customer has purchased or accesses Data Feeds, the content such feeds are provided solely on an "AS IS" and "AS AVAILABLE" basis and Everbridge disclaims any and all liability of any kind or nature resulting from (a) any inaccuracies or failures with respect to such Data Feeds or (b) any actions taken by Customer as a result of its use of the Solutions or its content. All Data Feeds are provided solely as a convenience and do not constitute an endorsement by Everbridge. The sole and exclusive remedy for any failure, defect, or inability to access the content of such Data Feed shall be to terminate the Data Feed with no further payments due. **"Data Feed"** means data content or websites licensed or provided by third parties to Everbridge and supplied to Customer in connection with the Solution (e.g., real time weather system information and warnings, 911 data, third party maps, and situational intelligence) or publicly available information that Customer accesses on the Internet while using the Services. Customers purchasing Visual Command Center or Signal products further agree that they will comply with the Data Feed Terms and Conditions found at https://www.everbridge.com/wp-content/uploads/Data-Feed-Terms-and-Conditions-Oct-2019.pdf.

8.7 Incident Management/IT Alerting. If Customer is purchasing the Incident Management or IT Alerting Solution, (a) Customer may only designate the number of Users set forth on the Order, and such individuals shall only have the access rights pursuant to such designation and role; (b) "Incident Administrators" are authorized by Customer as an administrator for the Incident Management or IT Alerting Solution components and are typically responsible for the configuration of IT Alerting as well as managing and reporting on Incidents; (c) "Incident Operators" are authorized by Customer as an operator of the Incident Management or IT Alerting Solution and are typically responsible for launching/managing Incidents; and (d) "Group Managers" shall have the ability to build, manage and/or participate in on-call schedules to receive IT related notifications. Everbridge may limit or throttle Customer's automated use of the Incident Management or IT Alerting Solution in order to protect the stability and security of the applicable Solution.

8.8 Secure Messaging. If Customer is purchasing peer-to-peer secure messaging solutions ("**Secure Messaging**"), Everbridge shall comply with all applicable privacy laws, including the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), the Health Information Technology for Economic and Clinical Health Act ("**HITECH Act**"), the Gramm-Leach-Bliley Act, and the Fair Credit Reporting Act, as applicable based on the Solution purchased. Everbridge's Secure Messaging products for healthcare are subject to the Everbridge Business Associate Agreement, available at https://www.everbridge.com/wp-content/uploads/2015/07/Business-Associate-Form-lkd-v1-7.7.15.pdf, which is incorporated and made a part of this Agreement. Customer acknowledges and agrees that Secure Messaging solutions are intended to deliver non-critical, non-emergency messages between users as a convenience to facilitate communications and are not intended for or suitable for use in situations where a failure or time delay of, or errors or inaccuracies in, the content, data or information provided through the services could lead to death, personal injury or property damage.

9. Non-Emergency Messaging. If Customer is using the applicable Solution to send non-emergency calls, text messages or emails to consumers, Customer expressly agrees to comply with the Telephone Consumer Protection Act of 1991, including its implementing regulations, the CAN-SPAM Act of 2003, and any other similar laws and regulation (collectively, "**Consumer Protection Law").** Customer shall not violate these or others applicable laws and warrants that it shall receive express consent from Contacts if its messages fall within these Consumer Protection Laws. Customer shall defend, indemnify and hold Everbridge harmless from any violation by Customer of Consumer Protection Law. Customer further agrees that any marketing or sales related text messages will comply with the policies and guidelines of the Mobile Marketing Association found at http://mmaglobal.com/policies/code-of-conduct.

10. Everbridge Service Levels.

Overview

This Service Level Agreement ("SLA") is applicable only to the provision of modules of Everbridge Suite, consisting of Mass Notification, Safety Connection, Incident Communications, IT Alerting, Crisis Management, and Visual Command Center (for purposes of this SLA, the "Services") that have been purchased by Customer. Everbridge reserves the right to change or update this SLA from time to time, except that such changes shall not reduce the targets set forth below. To the extent that there is any conflict between the terms of this SLA and the Agreement, the terms of the Agreement shall prevail.

Availability Target

Everbridge shall use commercially reasonable best efforts to achieve Availability of 99.99% or greater in each calendar quarter, with such quarters beginning as of 12:00 a.m. Pacific Standard Time on the first day of a given calendar quarter and ending at 11:59:59 p.m. Pacific Standard Time on the last day of a given calendar quarter.

"Availability" shall mean the ability to access the Services and send a notification to one or more delivery methods per recipient.

Performance Target

During a 60-minute period, Everbridge shall send a minimum number of messages to the first delivery method for all Customer notifications, using the standard configuration, per the table below. Messages do not include third party network delivery.

Delivery Method	Standard Message Configuration	Minimum Number of Messages in 60 Minutes
Everbridge smartphone application	500 characters	600,000
Voice	30 seconds	300,000
SMS	500 characters	600,000
Email	500 characters	600,000

Minimum numbers above do not apply when Customer uses the delivery throttling feature or intervals between delivery methods.

Scheduled Maintenance

"Scheduled Maintenance" means maintenance scheduled in advance to implement updates and/or perform system maintenance. In general, the timing of Scheduled Maintenance will be posted at least two (2) business days prior to the Scheduled Maintenance window. If Scheduled Maintenance is expected to interrupt Availability, then a Scheduled Maintenance service advisory will be posted to the Customer Support Center website.

Confidentiality

Customer acknowledges and agrees that this SLA and any information shared pertaining to this SLA shall constitute the Confidential Information of Everbridge. Customer's unauthorized disclosure of any such Confidential Information shall constitute a material breach of the Agreement. In the event of such material breach, Everbridge may exercise any rights provided in the Agreement or otherwise allowed by law. Customer's confidentiality obligations with respect to the SLA shall survive termination of the Agreement.

Reporting

Service level metrics will be provided quarterly upon request. Requests must be made in writing to Customer's Account Manager within fifteen (15) business days after the end of the applicable calendar quarter.

Everbridge Testing Methodology

For the purpose of establishing and measuring Availability, Everbridge regularly executes accessibility testing and measures success as an average percentage of uptime each quarter. The test utilizes an independent third-party solution to monitor the availability of Services from around the world. Availability is measured from multiple geographically distributed locations at multiple times per hour for all Services.

The Availability and Performance percentage is calculated by subtracting from 100% the percentage that the Services are determined not to be available or not performing in accordance with the target during a given calendar quarter. The quarterly Availability percentage shall be calculated only on the basis of whole calendar quarters.

SLA Exclusions

The targets set forth in this SLA do not apply in the event of disruptions caused by any (i) suspension of Services in accordance with the Agreement; (ii) factors outside of Everbridge's reasonable control, including force majeure event(s), or Internet access or related problems beyond the demarcation point of Everbridge; (iii) actions or inactions of the Customer or any third party, or (iv) Scheduled Maintenance.

SUPPLEMENTAL TERMS AND CONDITIONS (CAMMS/RISKONNECT GSP APPLICATIONS)

The following Additional Definitions, Additional Terms and Conditions and Additional Exhibits are incorporated into the Agreement by reference to the extent Customer has subscribed to one or more of the Riskonnect Applications as listed and described in a Subscription Order and/or SOW. All capitalized terms used but not otherwise defined in this Schedule A have the meanings set forth in the General Terms and Conditions, except as and to the extent amended below.

1. Additional Definitions:

1.1 "**Hosting Region**" means the hosting country (or countries) specified in the Subscription Order.

1.2 "**Licensors**" means, as applicable, depending on Customer's implementation of the Riskonnect Service:

1.2.1 Platform Provider.

1.3 "**Platform Provider**" means Microsoft Azure or Macquarie.

1.4 "**Platform Service**" means the online, web-based service provided by Platform Provider (as defined above) to Riskonnect in connection with Riskonnect's provision of the Riskonnect Service.

1.5 "**Riskonnect Locations**" means Australia, the United States, the United Kingdom, India, Sri Lanka, the Philippines and/or such other countries as Riskonnect may specify from time to time on reasonable notice.

1.6 "**User Information**" means the name, position, position description, location, email address, phone number and reporting officer of each User.

2. Additional Terms and Conditions.

2.1 **Usage Audit.** Riskonnect may remotely monitor Customer's usage of the Camms Applications to audit and verify Customer's compliance with the Agreement and any applicable usage restrictions. If an audit determines that Customer is not compliant with the Agreement, Customer shall reimburse Riskonnect, within thirty (30) days of the date of written notification of the audit results pay the additional fees for any usage in excess of Customer's rights under the Agreement (for which Riskonnect may immediately issue an invoice) and otherwise rectify the non-compliance to Riskonnect's reasonable satisfaction.

2.2 **Geographic Restrictions to Customer Data Access.** Riskonnect agrees to restrict geographic access to Customer Data as follows: (a) where the Subscription Order specifies that Customer is purchasing a 'Region Restricted' infrastructure security offering (which, as of the Effective Date, comprises Riskonnect's *Secure+, Protected+* or *Dedicated* options) then only Riskonnect personnel based in the Hosting Region specified in the Subscription Order may access Customer Data, and Riskonnect must not disclose, store, export or transfer Customer Data to a country outside the Hosting Region, *except that* Riskonnect may disclose User Information to employees and contractors of Riskonnect and its Affiliates who are based in Riskonnect Locations, solely for the purposes of providing the Riskonnect Service and Professional Services (and Customer acknowledges that Riskonnect personnel outside the Hosting Region may use the User Information to contact Users); (b) where the Subscription Order does not specify that Customer is purchasing a 'Region Restricted' infrastructure security offering, then Riskonnect may disclose, store, export or transfer Customer Data to a country outside the Hosting Region: (i) by giving remote access to Customer Data to employees and contractors of Riskonnect and its Affiliates who are based in Riskonnect Locations,

solely for the purposes of providing the Riskonnect Service and Professional Services; or (ii) with Customer's prior written consent.

2.3 **Data Deletion.** If Customer makes a request within two weeks of the effective date of termination of the Agreement or applicable Subscription Order, Riskonnect will deliver to Customer an electronic copy of the then most recent back-up of the Customer Data contained within the applicable Camms Application(s) hosted by Riskonnect, within two weeks of Customer's request. There is no charge for data export formats then commonly used by Riskonnect; if Customer requests different formats, Riskonnect may charge a fee. Riskonnect will delete the Customer Data in its possession within six months of the effective date of termination.

2.4 **Service Level Agreement**. The Service Level Agreement found at https://riskonnect.com/legal-sla/ is incorporated herein by this reference.

SCHEDULE B

AI and Data Usage Product Schedule

The following Additional Terms and Conditions are incorporated into the Agreement by reference to the extent Customer has subscribed to one or more of the modules within the Riskonnect Service as set forth on a Subscription Order and/or SOW that include any AI Features (as defined below), as well as any additional AI Features that are identified within the Riskonnect Service as containing AI Features. These Additional Terms and Conditions also govern Riskonnect's use of Customer Data in connection with Analytics Usage and Analytics Services (both as defined below).

"**AI Features**" means features or functions offered through a subscribed Riskonnect Service which use machine learning, predictive AI, and/or generative AI technologies, and are specified in the relevant Subscription Order or SOW or identified as containing AI functionality within the Riskonnect Service itself.

Additional Terms and Conditions

1. AI FEATURES

1.1 AI Features may be available to Customer through an existing Riskonnect Service entitlement at no additional charge ("**Included AI Features**"), or they may be paid-for additional features ("**Paid AI Features**"). Riskonnect will enable Paid AI Features following Customer's execution of the applicable Subscription Order and/or SOW for those Paid AI Features. Riskonnect will not enable Included AI Features automatically, and Customer must specifically request that they be enabled. Customer may also request that one or more AI Features be disabled for its account at any time. Customer is not entitled to any refund for Paid AI Features which are disabled at Customer's request.

1.2 Any third-party providers of an AI Feature ("**Third-Party Model Providers**", which shall also be deemed Licensors for all purposes under the Agreement) are included in the list of subprocessors referenced in the applicable Data Processing Agreement ("**DPA**") or are otherwise identified in this Product Schedule. Riskonnect has entered into appropriate contractual terms with such Third-Party Model Providers to ensure that Customer Data submitted to such providers is adequately protected in accordance with Data Protection Laws and Regulations as further detailed in the applicable DPA.

1.3 Riskonnect reserves the right to modify or discontinue any AI Features at any time to ensure compliance with applicable laws, regulations, and guidance relating to the secure, ethical, and responsible use of AI technologies.

2. OWNERSHIP

2.1 For the purposes of this Product Schedule, a "**Prompt**" is any command, instruction, or query submitted to an AI Feature to trigger a function or produce Output. A "**Riskonnect Derived Prompt**" is a Prompt created by an AI Feature, consisting of a Prompt template developed by Riskonnect. A "**Customer-Owned Derived Prompt**" is a Prompt created by an AI Feature consisting of Customer Data and/or Prompts that are created, customized,

or owned by Customer for their specific use within the AI Features. A Riskonnect Derived Prompt and a Customer-Owned Derived Prompt shall together be referred to in this Product Schedule as a "**Derived Prompt**." "**Output**" means the results or deliverables generated by the AI Feature in response to a Prompt, including but not limited to data, reports, insights, or any other content produced by the AI Features.

Ownership of Prompts

2.2 Customer owns all rights, title, and interest in and to the Customer-Owned Derived Prompts.

2.3 Riskonnect owns all rights, title, and interest in and to the Riskonnect Derived Prompts, which shall be included in the definition of Riskonnect Service for all purposes under the Agreement.

2.4 As between the Parties, Customer will exclusively own all Outputs, and Riskonnect hereby assigns to Customer and its successors, without separate consideration, all rights, title, and interest that Riskonnect may now or hereafter have in and to the Outputs throughout the world, including, without limitation, all Intellectual Property Rights in and to the Outputs.

2.5 Nothing in this Product Schedule shall transfer or assign to either Party any ownership rights in the other Party's proprietary models, templates, or algorithms beyond the license rights expressly granted herein.

2.6 Customer hereby grants to Riskonnect a worldwide non-exclusive, royalty-free, fully paid-up, license to use, reproduce, modify, distribute, and display all Prompts and Output in connection with the provision of services under the Agreement.

3. AI FEATURE USE AND COMPLIANCE

3.1 Customer shall, at all times, ensure that its Users use the AI Features solely in accordance with the intended purposes and functionalities thereof, and with the limitations set forth in this Product Schedule. In addition to the User restrictions contained in the Agreement, Customer shall not and shall ensure that its Users do not:

3.1.1 use the AI Features other than as expressly authorized and described within the particular AI Feature;

3.1.2 attempt to circumvent or bypass any limitations or restrictions implemented by Riskonnect;

3.1.3 use the AI Features as a substitute for, or to otherwise circumvent the need for, human judgment or expertise in any decision-making process where such human judgment or expertise is legally required or is otherwise reasonably necessary to protect the health, safety, or fundamental rights of any natural person;

3.1.4 use the AI Features for the purpose of categorizing, profiling, or discriminating against any natural person on the basis of any actual or inferred characteristic that is protected by law from such categorization, profiling, or discrimination, including but not limited to race, ethnicity, gender, religion, sexual orientation, or disability;

3.1.5 use the AI Features to predict, assess, or evaluate any natural person's propensity toward criminal or dishonest behavior, or for any purpose related to risk assessment, security vetting, or law enforcement, unless expressly authorized by Riskonnect in writing; and

3.1.6 use the AI Features in any way that does not comply with all other laws, rules, and regulations applicable to customer including but not limited to Data Protection Laws and Regulations and those laws and regulations related to artificial intelligence.

3.2 Riskonnect represents, and Customer acknowledges and agrees, that based on Riskonnect's good faith assessment of the proposed EU Artificial Intelligence Act (the "**AI Act**") as of the date of this Agreement, the AI Features are designed and intended to function in a manner such that they would not be classified as "high-risk AI systems" or "General Purpose AI systems" under that AI Act. Customer warrants that it shall not use the AI Features in any manner that contradicts or undermines this representation and shall implement and maintain all reasonable and necessary safeguards to prevent such use, including but not limited to providing adequate training to its Users, monitoring User activity, and implementing appropriate technical and organizational measures.

3.3 Without prejudice to its other rights under the Agreement or at law, Riskonnect reserves the right to disable Customer's access to AI Features if it considers in good faith that it is necessary to stop or to prevent breach of this Section 3.

4. THIRD-PARTY API USE AND CUSTOMER RESPONSIBILITIES

4.1 Customer agrees to the additional terms and conditions in the attached **Exhibit 1**, that apply to Customer's use of the AI Features that are provided by Third-Party Model Providers, as applicable:

4.2 Customer hereby consents to the following Third-Party Model Providers as Licensors and as subprocessors for purposes of processing Personal Data in connection with Customer's use of the AI Features (to the extent applicable):

4.2.1 OpenAI (United States)

4.2.2 Microsoft Azure (Australia, Canada, EU, India, South Africa, South America, South Asia, UAE, United Kingdom, United States)

4.2.3 Salesforce (Australia, Ireland, Singapore, United States)

4.3 In addition, Customer hereby consents to the following Licensors as subprocessors for purposes of processing Personal Data in connection with Customer's use of the AI Features, as well as Riskonnect's reporting and analytics services (including Analytics Usage, as defined below) to the extent licensed under an applicable Subscription Order.

4.3.1 Power BI (Australia, Canada, EU, India, South Africa, South America, South Asia, UAE, United Kingdom, United States)

4.3.2 Striim (Australia, Canada, EU, India, South Africa, South America, South Asia, UAE, United Kingdom, United States)

4.4 If Customer supplies its own API keys in order to access and use an AI Feature, Customer shall be solely responsible for compliance with the policies, terms and applicable laws related to the use of that AI Feature. Customer shall notify Riskonnect promptly if it is in breach of those terms and/or ceases to have access to such AI Feature, and in such an event, Riskonnect shall promptly disable access to such AI Feature. Riskonnect shall not be liable for any damages, claims, or losses relating to Customer's use (whether the AI Feature is accessed via Riskonnect's API keys or directly with their own API keys) of third-party APIs.

5. CUSTOMER SHALL INDEMNIFY, DEFEND, AND HOLD RISKONNECT, ITS AFFILIATES AND EMPLOYEES HARMLESS FROM AND AGAINST ANY CLAIMS, DAMAGES, PENALTIES, OR LEGAL ACTIONS ALLEGING (1) THAT CUSTOMER IS IN VIOLATION OF ANY THIRD PARTY MODEL PROVIDER'S TERMS OF USE AS REFERENCED HEREIN, OR (2) THAT CUSTOMER'S USE OF THE AI FEATURES, PROMPTS, OR OUTPUT VIOLATES ANY APPLICABLE LAW.

6. TRANSPARENCY AND RESPONSIBLE USE

6.1 As between Riskonnect and Customer, Customer is solely responsible for all required disclosures to and obtaining appropriate consents from natural persons affected by Customer's use of AI Features.

6.2 Riskonnect or Third Party Model Providers may publish notice, with requirements for use of an AI Features, within the applicable AI Feature or Riskonnect Service certain transparency information and/or additional guidance on use regarding intended functionality and acceptable uses of AI Features to ensure Customer's use of the applicable AI Features is in accordance with applicable laws. Notwithstanding anything to the contrary in the Agreement, Customer hereby accepts and agrees to comply with such terms.

6.3 Each Party shall take appropriate and necessary measures to ensure that its personnel and any Users involved in the provision or use of AI Features, have a sufficient level of "AI literacy" in accordance with the AI Act.

7. RETENTION

7.1 If applicable, Output and Prompts may be retained within the AI Feature or stored by Third-Party Model Providers. Such Output and Prompts shall be securely deleted or anonymized promptly in accordance with Riskonnect's and the Third-Party Model Provider's data retention policies and procedures but in any event in compliance with applicable law or regulation. Any Output stored in the Riskonnect Service other than an AI Features shall be Customer Data, and its retention and deletion handled in accordance with the Agreement or the applicable Product Schedule.

7.2 Cessation of access to the AI Features or termination of this Agreement shall result in the deletion or anonymization of all retained Output containing Customer Data, unless a longer retention period is required by law or regulation.

8. DATA PROTECTION

8.1 In processing any Personal Data contained within Customer Prompts, Customer-Owned Derived Prompts, or Customer Output, Riskonnect acts as Customer's processor, in accordance with the applicable data protection provisions of the Agreement, or the applicable DPA or BAA, as the case may be. In processing Personal Data in order to produce anonymized data sets for Development Usage (as defined below), Riskonnect acts as controller. However, because Riskonnect has no direct contact with the data subjects concerned, it is Customer's responsibility to ensure that it has provided the necessary information to those data subjects (including a point of contact at Customer) and obtained all required consents and/or established all required legal bases for such processing, and to ensure that Riskonnect is promptly informed of any data subject objections or requests to exercise their rights in respect of their Personal Data as processed by Riskonnect for that purpose.

9. OPT-IN TO DEVELOPMENT USAGE OF ANONYMIZED CUSTOMER DATA

9.1 With Customer's prior written consent (which may be indicated on the relevant Subscription Order or otherwise explicitly agreed in writing), Riskonnect and/or its Affiliates may use Customer's Prompts and Output internally for the exclusive purposes of developing, training, testing, and enhancing existing and future AI Features ("**Development Usage**"). Such use shall only involve anonymized data that does not identify Customer or any natural person.

9.2 Customer may withdraw its consent to the Development Usage of Prompts and Output at any time by providing written notice to Riskonnect. Upon receipt of such notice, Riskonnect shall cease using Customer's Prompts and Output for Development Usage within a commercially reasonable time frame, not exceeding thirty (30) days. The withdrawal of consent shall not affect the legality of any Processing conducted prior to the withdrawal.

9.3 Customer warrants that it possesses all necessary rights in the Prompts and Customer Output to grant this consent and confirms that it has complied with all Data Protection Laws and Regulations, including the anonymization of any Personal Data as outlined in Section 8.1.

9.4 Riskonnect shall adopt and maintain appropriate technical and organizational measures to ensure that all Customer Data used for Development Usage is protected against unauthorized access, loss, disclosure, alteration, or destruction, in accordance with industry standards. Riskonnect shall ensure that such data is anonymized through accepted de-identification techniques so that it does not directly or indirectly identify Customer or any natural person. The use of Customer Data for Development Usage shall be limited to internal purposes related to the development, training, testing, and refinement of AI Features, and Riskonnect shall not knowingly disclose or transfer anonymized Customer Data to any third parties, including external vendors or third-party AI systems, except as expressly permitted under this Agreement or by applicable law.

9.5 By agreeing to use the AI Features, Customer acknowledges these measures and Riskonnect's commitment to adhere to its obligations under Data Protection Laws and Regulations. Certain AI Features, such as those providing predictions based on large multi-sourced datasets, may require Customer's agreement to Development Usage in respect of that AI Feature or the associated Riskonnect Application as a condition of access to that AI Feature.

10. OPT-IN TO ANALYTICS USAGE OF ANONYMIZED CUSTOMER DATA

10.1 Riskonnect and/or its Affiliates may collect and process information about Customer's use of the Riskonnect Service, may analyze and aggregate such data and information with data and/or information Riskonnect may have obtained or may in the future obtain from other of its customers, publicly available sources and/or data providers, and may disclose such analyses and aggregated data to individual prospective or current customers, provided that (i) such data is aggregated and de-identified prior to such use, (ii) Riskonnect does not use such aggregated and de-identified data in a manner which would allow identification of Customer or individuals, and (iii) Customer Data is not transferred to such prospective or current customers ("**Analytics Usage**"). Customer agrees that Riskonnect or its Affiliates may use aggregated and de-identified data for these purposes.

10.2 Customer may withdraw its consent to the Analytics Usage of Customer Data at any time by providing written notice to Riskonnect. Upon receipt of such notice, Riskonnect shall cease using Customer Data for Analytics Usage within a commercially reasonable time frame, not exceeding thirty (30) days. The withdrawal of consent shall not affect the legality of any Processing conducted prior to the withdrawal.

a. Customer acknowledges and agrees that Analytics Usage will be based upon a number of assumptions, conditions and factors. If any of them or any information provided to Riskonnect is inaccurate or incomplete or should change, any services provided by

Riskonnect involving Analytics Usage ("**Analytics Services**") could be materially affected. Analytics Usage is subject to inherent uncertainty, and actual results may differ materially from those projected by Riskonnect. Analytics Services are provided solely for the Customer's benefit, and do not constitute, and are not intended to be a substitute for, actuarial, accounting or legal advice. Riskonnect shall have no liability to any third party in connection with the Analytics Services or to Customer regarding such services performed or provided by a third party.

11. DISCLAIMER

RISKONNECT MAKES NO REPRESENTATIONS OR WARRANTIES THAT ANY OUTPUT, RISKONNECT PROMPTS, OR AI FEATURES DO NOT INCORPORATE OR REFLECT THIRD-PARTY CONTENT OR MATERIALS, OR THAT THEY WILL NOT INFRINGE THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS. NOTWITHSTANDING ANY OTHER PROVISIONS IN THE AGREEMENT, RISKONNECT SHALL NOT BE OBLIGATED TO DEFEND, HOLD HARMLESS, OR INDEMNIFY CUSTOMER OR USER AGAINST ANY CLAIMS, INCLUDING THIRD-PARTY INFRINGEMENT CLAIMS, ARISING FROM USE OF OUTPUTS OR AI FEATURES. OUTPUT MAY NOT BE ERROR FREE OR UP TO DATE AND RISKONNECT MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY, COMPLETENESS OR TIMELINESS OF THE OUTPUT. ALL OUTPUT IS PROVIDED TO CUSTOMER "AS IS" WITH NO REPRESENTATION OR WARRANTY OF ANY KIND, INCLUDING BUT NOT LIMITED TO FITNESS FOR A PARTICULAR PURPOSE AND/OR MERCHANTABILITY. RISKONNECT DISCLAIMS ALL LIABILITY FOR CUSTOMER'S USE AND RELIANCE ON OUTPUT.

12. INDEMNIFICATION

Customer shall defend, indemnify and hold harmless Riskonnect, its Affiliates from and against any and all damages, liabilities, claims, costs, fines, penalties, judgments, settlements, and expenses (including reasonable attorneys' fees and court costs) incurred by an indemnified Party arising out of or relating to Customer's breach of Sections 3 (*AI Feature Use and Compliance*), 6 (*Transparency and Responsible Use*) and 8 (*Data Protection*).

Exhibit 1

A. **Open AI**

1. Customer agrees to OpenAI Terms of Use (where Customer shall be considered an End User) at https://openai.com/policies/terms-of-use.

2. If the AI Feature uses OpenAI's API, Customer acknowledges that OpenAI may process information derived from Prompts and Output that has been de-identified, anonymized, and/or aggregated so that it is no longer considered Personal Data under applicable Data Protection Laws. This processing occurs in a manner that does not identify individuals or Customer and is solely to improve OpenAI's systems and services.

B. **Power BI**

1. If Customer has subscribed or has access to an AI Feature that utilizes the Power BI API, Customer agrees that neither it nor its Users will:

a. defame, abuse, harass, stalk, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of others;
upload, post, email or transmit or otherwise make available any inappropriate, defamatory, infringing, obscene, or unlawful content;
b. upload, post, email or transmit or otherwise make available any content that infringes any patent, trademark, copyright, trade secret or other proprietary right of any party, unless you are the owner of the rights or have the permission of the owner to post such content;
c. upload, post, email or transmit or otherwise make available messages that promote pyramid schemes, chain letters or disruptive commercial messages or advertisements, or anything else prohibited by law, these API Terms or any applicable policies or guidelines;
d. use the Power BI API in connection with or to promote any products, services, or materials that constitute, promote or are used primarily for the purpose of dealing in: spyware, adware, or other malicious programs or code;
e. download any file posted by another that you know, or reasonably should know, that cannot be legally distributed in such manner;
f. impersonate another person or entity, or falsify or delete any author attributions, legal or other proper notices or proprietary designations or labels of the origin or source of software or other material;
g restrict or inhibit any other user from using and enjoying access to Power BI API;
h use Power BI API for any illegal or unauthorized purpose;
i. remove any copyright, trademark or other proprietary rights notices contained in or on Power BI API;
j. interfere with or disrupt Power BI API or servers or networks connected to Power BI services, or disobey any requirements, procedures, policies or regulations of networks connected to Power BI API;
k. use any robot, spider, site search/retrieval application in relation to Power BI API or collect information about users for any unauthorized purpose;
l. submit content that falsely expresses or implies that such content is sponsored or endorsed by Microsoft;

m. create user accounts by automated means or under false or fraudulent pretenses, or obtain or attempt to obtain multiple keys for the Power BI API;
n. promote or provide instructional information about illegal activities or promote physical harm or injury against any group or individual; or
o. transmit any viruses, worms, defects, Trojan horses, or any items of a destructive nature.
p. sell, lease, share, transfer, or sublicense the Power BI API or access codes thereto, whether for direct commercial or monetary gain or otherwise, without Microsoft's prior, express, written permission; or
q. use the Power BI API in a manner that exceeds reasonable request volume, constitutes excessive or abusive usage, or otherwise fails to comply or is inconsistent with any part of the Power BI API documentation located within dev.PowerBI.com as determined by Microsoft in its sole discretion;
r. request data on behalf of one user in order to show, display, transmit, or deliver such data to other users;
s. ensure that all Customer Data and documents provided to Power BI shall not contain any virus, works, harmful scripts or code, or other malware.

2. Customer will indemnify and hold Microsoft (and its directors, officers, affiliates, and agents) harmless from, and against, any and all loss, liability, and expense (including reasonable attorneys' fees and costs) suffered or incurred by reason of any claims, proceedings, or suits based on or arising out of any breach (or alleged breach) of the Terms of Use contained herein by Customer with respect to its use of Power BI. Customer will be solely responsible for defending any such claim using mutually-agreed counsel, subject to Microsoft's right to participate with counsel it selects, and Customer will not publicize any claim or agree to any settlement that imposes any obligation or liability on Microsoft (or its directors, officers, affiliates, and agents) without Microsoft's prior written consent, such consent provided by Microsoft in its sole discretion.

3. THE POWER BI API IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS WITH NO WARRANTY, EXPRESS OR IMPLIED, OF ANY KIND. MICROSOFT EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES AND CONDITIONS, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AVAILABILITY, SECURITY, TITLE AND NON-INFRINGEMENT. YOUR USE OF THE POWER BI API IS AT YOUR OWN DISCRETION AND RISK, AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE THAT RESULTS FROM THE USE OF POWER BI API.

4. MICROSOFT DOES NOT REPRESENT OR WARRANT THAT THE POWER BI API IS FREE OF INACCURACIES, ERRORS, BUGS, OR INTERRUPTIONS, OR IS RELIABLE, ACCURATE, COMPLETE, OR OTHERWISE VALID. MICROSOFT MAKES NO WARRANTY THAT (i) THE POWER BI API WILL MEET YOUR REQUIREMENTS, (ii) THE ACCESS TO POWER BI API SERVICE WILL BE UNINTERRUPTED, (iii) THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE POWER BI API WILL BE ACCURATE OR RELIABLE, (iv) THE QUALITY OF ANY PRODUCTS, SERVICES, INFORMATION, OR OTHER MATERIAL OBTAINED BY YOU THROUGH THE POWER BI API WILL MEET YOUR EXPECTATIONS, AND (v) ANY ERRORS IN THE POWER BI API WILL BE CORRECTED.

C. **Salesforce Agentforce**

This Exhibit incorporates Salesforce SFDC Terms of Use for OEM Partners as pass-through terms. Full terms are available at https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/Agreements/alliance-agreements-and-terms/OEM-Pass-Through-Terms.pdf.

EXHIBIT A
STATEMENT OF WORK

[PLACEHOLDER FOR STATEMENT OF WORK]

EXHIBIT B
SUBSCRIPTION ORDER

[PLACEHOLDER FOR SUBSCRIPTION ORDER]

EXHIBIT C
SECURITY EXHIBIT

ACTIVE RISK MANAGER (ARM) AND RESILIENCE PRODUCTS

1. LOGICAL ACCESS CONTROL

a. Access

i. Riskonnect denies all access to information systems and resources by default. Access is granted by request for specific business purposes, and in accordance with the principles of least privilege and separation of duties. Riskonnect controls the use of administrative privileges by tracking, preventing, and correcting the use, assignment, and configuration of administrative privileges on computers, networks, and applications through a formal access recertification process.

ii. Riskonnect maintains appropriate usage restrictions and configuration/connection requirements for information systems (including wireless) access, which requires prior authorization for access to the systems prior to allowing such connections. All access to Riskonnect's information systems and resources requires management approval.

iii. Riskonnect maintains appropriate usage restrictions, configuration/connection requirements, and implementation guidance for organization-controlled mobile devices, and authorizes (as described above) the connection of mobile devices to organizational information systems.

b. Account Management. Riskonnect configures its information systems and resources to enforce access control policies and standards and requires or forces users to log out after a pre-determined amount of inactivity.

2. AWARENESS AND TRAINING

a. Security Awareness Training

i. Riskonnect maintains, regularly reviews, documents, and administers security awareness training for all of Riskonnect's personnel.

ii. Training is administered as part of the new hire onboarding process and annually thereafter.

3. AUDIT AND ACCOUNTABILITY

a. Audit Logs. Riskonnect's information systems will generate audit logs containing the type of event, the date and time of the event, the location of the event, the source of the event, the outcome of and response to the event, the individual(s) associated with the event and any other information relevant to the event and provide such information to Customer upon request.

b. System Logging and Review

i. Riskonnect's information systems protect audit information, including audit records, audit settings, audit reports, and audit tools from unauthorized access, modification, and deletion. Audit information must be backed up onto a physically different system or system component than the system or component being audited. Riskonnect's information systems

implement cryptographic protection to ensure the integrity of audit information and enforce the principles of separation of duties and least privilege in the review, analysis, and reporting of audit records.

ii. Riskonnect retains audit logs to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

iii. Depending on the relevant hosting environment in which the Riskonnect Application will reside, and Customer Data will be processed, and as detailed in the applicable Product Schedule, such hosting environment will **(a)** be subject to an annual SOC2 Type2 audit or **(b)** have achieved ISO 27001 certification. Additionally, as part of the annual SOC2 Type2 audit or ISO 27001 certification process, Riskonnect engages a qualified third party to conduct an audit of, and perform penetration testing on, the subject hosting environment. In lieu of authorizing Customer to conduct its own audit or penetration testing of the subject hosting environment (but subject to a requirement under applicable law for Customer to have such audit conducted) and upon Customer's written request, Riskonnect will deliver to Customer: **(1)** as applicable, a copy of its latest SOC 2 Type2 report and/or a copy of its latest ISO 27001 or ISO 22301 certificate; and **(2)** a summary of the related annual penetration testing results. Finally, Riskonnect will respond to additional Customer information security questionnaires so long as such questionnaires are **(i)** submitted to Riskonnect not more than once per twelve (12) month time period and **(ii)** limited to using either the SIG Lite or CAIQ format.

4. SECURITY ASSESSMENT AND AUTHORIZATION

a. Security Authorization. Riskonnect assigns a senior-level executive or manager as the authorizing official for the information systems, ensures that such official authorizes the information systems for processing before commencing operations, and periodically updates the security authorization as needed.

b. Continuous Monitoring. Riskonnect maintains a Data Loss Prevention ("**DLP**") strategy to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. Riskonnect maintains a continuous monitoring program that includes establishing metrics to be monitored, the frequency for monitoring, response actions to address the results of such analysis, and reporting the security status of the Riskonnect information system to the appropriate personnel.

5. CONFIGURATION MANAGEMENT

a. Information System Component Inventory. Riskonnect develops, documents, and regularly updates an inventory of information system components. Riskonnect detects, tracks, and restricts all hardware devices on its non-public networks so that only authorized devices are given access, and detects, tracks, and restricts all software on such networks so that only authorized software is installed.

b. Configuration Management Plan. Riskonnect establishes and implements a configuration management plan, employing the principle of least functionality. Riskonnect establishes, implements, and actively tracks, corrects, and reports on the security configuration of network infrastructure devices using a rigorous configuration management and change control process that are reasonably designed to prevent attackers from exploiting vulnerable services and

settings. The configuration management plan addresses roles and responsibilities and flaw remediation, as well as defines detailed processes and procedures for how configuration management is used to support Riskonnect's system development lifecycle. The plan describes how to move changes through the system, how to update baselines and configuration settings, how to maintain system component inventories, and how to control development, test, and operational environments.

c. **Baseline Configuration and Hardening.** Riskonnect develops, documents, and maintains current baseline configuration and hardening requirements for Riskonnect's information systems. Baseline configurations and hardening requirements are reviewed and updated regularly and as part of information system component installations and updates. Security compliance assessments are performed on new servers and applications prior to migration into production and repeated periodically based on risk to ensure compliance with Riskonnect's system hardening requirements. Riskonnect retains previous versions of baseline configurations of the information systems to support rollback and maintains a baseline configuration for information system development and test environments that are managed separately from the operational baseline configuration.

d. **Configuration Change Control.** Riskonnect establishes and implements a formal change control process designed to prevent unauthorized changes and documents all changes to network infrastructure. Riskonnect tests, validates, and documents changes to the information systems before implementing the changes on the operational systems, and requires that an information security representative be a member of the configuration change control team.

6. CONTINGENCY PLANNING

a. **Contingency Plan.** Riskonnect develops a contingency plan for the information systems, which identifies essential business missions/functions and associated contingency requirements, provides recovery objectives and restoration responses, addresses contingency roles and responsibilities, addresses maintaining essential business functions in the event of system disruption or failure, and addresses full system restoration without deterioration of the security safeguards in place. The contingency plan is regularly reviewed and updated at least annually, and as needed to address changes in the threat environment.

b. **Information System Backup and Alternate Storage Site.** Riskonnect conducts backups of user-level information, system-level information, and system documentation including security-related documentation. Riskonnect maintains alternate storage locations permitting storage and prompt retrieval of information system backup information. Storage of information system backups are protected with information security safeguards of an equivalent strength to that of the primary system and storage site.

c. **Information System Recovery and Reconstitution.** Riskonnect promptly provides for the recovery and reconstitution of information systems to a state of normal operation after disruption, compromise, or failure. This recovery plan includes transaction-based recovery, and protects backup and restoration hardware, software, and firmware.

7. IDENTIFICATION AND AUTHENTICATION

a. Unique Identification. Riskonnect's information systems uniquely identify and authenticate both organizational and non-organizational users and/or processes acting on behalf of users, such that all user activity can be traced back to the individual(s) who performed the activity. Riskonnect's systems employ industry standard encryption for all authentication mechanisms, provide for federated identity capabilities, and implement replay-resistant authentication mechanisms. Information systems implement multifactor authentication for network and local access to both privileged and non-privileged accounts.

b. Non-Repudiation. Riskonnect's information systems enforce non-repudiation such that the validity and authenticity of an action or task cannot be disputed, including creating and/or changing information, sending and receiving messages, approving information, signing contracts, and approving procurement requests.

c. Device Identification and Authentication. Devices attempting to access Riskonnect's network are uniquely identified and authenticated via a Network Access Control system (or other comparable means) prior to establishing a network connection.

d. Authentication Management. Riskonnect manages information system credentials/authenticators using industry best practices. Riskonnect takes into consideration the type of authentication (e.g., hardware token-based, PKI-based, password-based, biometric-based, etc.) and applies additional security controls as appropriate.

8. INCIDENT RESPONSE

a. Incident Response Program. Riskonnect maintains a written incident response program that addresses cybersecurity event preparation, detection, analysis, containment, eradication, and recovery. This program includes procedures that describe: **(i)** roles and responsibilities of the incident response team; **(ii)** communication requirements with internal and external partners; **(iii)** plans to detect, respond to, and contain common incident categories; **(iv)** methods to preserve evidence, maintain chain of custody, and perform forensic analysis; **(v)** coordination of recovery processes; **(vi)** follow-up processes; and **(vii)** reporting to ensure critical details of incidents are tracked and lessons learned are incorporated into ongoing response procedures, training, and testing. The incident response program includes coordinating incident handling activities involving supply chain events with other organizations involved in the supply chain. The incident response program is reviewed and updated at least annually.

b. Incident Handling. If Riskonnect discovers or is notified of any security incident that impacts or may impact Customer Data and/or systems, Riskonnect will promptly: **(i)** investigate the security incident; **(ii)** remediate, mitigate, or remediate and mitigate, the risk to the Customer Data or systems and other effects of the security incident; **(iii)** preserve all related records and other evidence; and **(iv)** implement a plan to prevent such a security incident from reoccurring.

c. Incident Notification. If Riskonnect discovers or is notified of any security incident, Riskonnect will immediately notify Customer thereof in writing, but no later than seventy two (72) hours from the time Riskonnect becomes aware of a security incident, including disclosing **(i)** the date, time, and cause of the incident if known; **(ii)** the Customer Data and/or systems that were exposed or

reasonably believed to have been exposed; and **(iii)** whether nonpublic personally identifiable information was accessed.

d. Reporting. Riskonnect will provide Customer with a written report on the outcome of its investigation including any risk to Customer Data and/or systems, the corrective action Riskonnect has taken to respond to the security incident, and such other information as Customer may reasonably request regarding the security incident.

9. MAINTENANCE

a. Nonlocal Maintenance. Riskonnect: **(i)** approves, documents, and monitors nonlocal maintenance and diagnostic activities; **(ii)** allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; **(iii)** requires multifactor authentication to establish nonlocal maintenance and diagnostic sessions via external network connections; **(iv)** maintains records for nonlocal maintenance and diagnostic activities; and **(v)** terminates session and network connections when nonlocal maintenance is completed. Riskonnect protects nonlocal maintenance sessions by employing replay-resistant authenticators and separating the maintenance sessions from other network sessions by either physically or logically separated communication paths based on encryption.

b. Timely Maintenance. Riskonnect approves, obtains, and documents the maintenance, support, and repair of information systems and information system components in a timely manner following system or component failure. Riskonnect performs preventative maintenance on critical information system components at regular intervals, or as needed, to ensure that they are in operating condition. Security controls potentially impacted during maintenance or repair activities are inspected for proper function post-activity. Riskonnect promptly applies software patches, updates, and code fixes, when available.

10. MEDIA PROTECTION

a. Media Use. Riskonnect employs both technical and non-technical safeguards to restrict the use of removable media and portable storage devices.

b. Media Storage. Riskonnect physically controls and securely stores both digital and non-digital media and protects information system media until such media are destroyed or sanitized using secure data destruction techniques. Riskonnect restricts access to media storage areas and maintains access logs for both successful and unsuccessful access attempts.

c. Media Transport. Riskonnect: **(i)** protects and controls information system media during transport outside of controlled areas using physical and technical safeguards; **(ii)** maintains accountability for information system media during transport outside of controlled areas; **(iii)** documents activities associated with the transport of information system media; and **(iv)** restricts the activities associated with information system media to authorized personnel. Information systems implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

d. Media Sanitization. Riskonnect sanitizes information system media prior to disposal, release from organizational control, or release for reuse in accordance with organizational policies, employing sanitation mechanisms with the strength and integrity commensurate with the security category

or classification of the information. Riskonnect: **(i)** reviews and approves media to be sanitized to ensure effectiveness and compliance with records-retention policies and **(ii)** tracks and documents the media sanitation process, including personnel who handled such media, and verifies that that sanitation of the media was effective prior to disposal. The information systems, system components, and system devices are capable of being purged/wiped remotely to protect data obtained by unauthorized individuals.

11. PHYSICAL AND ENVIRONMENTAL PROTECTION

a. **Physical Access Control.** Riskonnect: **(i)** enforces physical access authorizations at facility entrance/exit points by verifying individual access authorizations before granting access to the facility; **(ii)** maintains physical access audit logs for entry/exit points; and **(iii)** uses security safeguards to control access of such facilities, including the use of security guards (only at data processing facilities where the Riskonnect Service resides) and physical access control devices (e.g., alarms, card swipe, keypads).

b. **Power Equipment and Cabling.** Riskonnect protects power equipment and cabling for the information systems from damage and destruction. Riskonnect employs physically separate, redundant power cables to ensure that power continues to flow if one cable is cut or otherwise damaged, as well as automatic voltage controls for critical information system component.

c. **Location of Information System Components.** Riskonnect positions information system components within the facility to minimize potential damage from environmental hazards (e.g., flooding, fire, tornados, earthquakes, hurricanes, vandalism, acts of terrorism, electromagnetic pulse, electrical interference, etc.) as well as physical hazards, including the opportunity for unauthorized access.

12. PLANNING

a. **Information Security Architecture.** Riskonnect maintains information security architecture for the information systems that includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The information security architecture is reviewed and updated regularly to reflect updates in the enterprise architecture, external impacts, and industry practices. These changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

13. PERSONNEL SECURITY

a. **Personnel Screening.** Riskonnect screens individuals prior to authorizing access to Riskonnect's information systems), including background checks.

b. **Personnel Termination.** Upon termination, Riskonnect promptly: **(i)** disables the individual's information system access; **(ii)** terminates/revokes any authenticators/credentials associated with the individual; **(iii)** conducts exit interviews that include information security topics; **(iv)** retrieves all security-related organizational information system-related property (e.g., hardware authentication tokens, system administration technical manuals, keys, identification cards, building passes, etc.); and **(v)** retains access to organizational information and information systems formerly controlled by terminated individual.

14. RISK ASSESSMENT

a. Risk Assessment. Riskonnect: **(i)** conducts a risk assessment, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information systems and the information they process, store, or transmit; **(ii)** documents and reviews the risk assessment results; and **(iii)** updates the risk assessment regularly, and whenever there are significant changes to the information system or environment of operation (e.g. the identification of new threats and vulnerabilities).

b. Vulnerability Scanning. Riskonnect: **(i)** scans for vulnerabilities in the hosted application at least annually and when new vulnerabilities potentially affecting the system/applications are identified; **(ii)** employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for enumerating platforms, software flaws, and improper configurations, formatting checklists and test procedures, and measuring vulnerability impact ; **(iii)** analyzes vulnerability scan reports and results from security control assessments; **(iv)** remediates vulnerabilities in accordance with organizational risk assessment; **(v)** shares information from the vulnerability scanning and security control assessments with appropriate personnel to help eliminate similar vulnerabilities in other information systems; and **(vi)** employs periodic external vulnerability scanning and annual penetration testing to assess the overall strength of Riskonnect's defenses (technology, processes, and employees). Upon Customer's written request, Riskonnect will deliver to Customer a summary of the results of the most recent vulnerability scans and penetration tests.

15. SYSTEM DEVELOPMENT LIFE-CYCLE

Riskonnect manages information systems using industry standard System Development Life Cycle ("**SDLC**") that incorporates information security considerations, defines and documents information security roles and responsibilities throughout the SDLC, identifies individuals having such roles or responsibilities, and integrates Riskonnect's information security risk management process into SDLC activities.

16. SUPPLY CHAIN RISK MANAGEMENT

Riskonnect **(i)** protects against supply chain threats to the information systems, components, or service by employing security safeguards as part of a comprehensive information security strategy, including the use of secure acquisition strategies, contract, tools, and procurement methods for purchasing of information systems, components, and services from suppliers; **(ii)** conducts supplier reviews prior to engaging into a contractual agreement to acquire information systems, components, or services; **(iii)** maintains security safeguards to limit harm from potential adversaries targeting the organizational supply chain; and **(iv)** conducts assessments of the information systems, components, or services prior to selection, acceptance, or update.

17. SYSTEMS AND COMMUNICATIONS PROTECTION

a. Boundary Protection. Riskonnect **(i)** monitors and controls communications at the external boundaries and at key internal boundaries of the organizational system; **(ii)** implements sub-networks for publicly accessible system components that are physically or logically separated from internal networks; **(iii)** limits the number of external network connections; and **(iv)** employs a deny by default, permit by exception policy for network communication traffic for both inbound and outbound communications. Riskonnect networks, and connects to external networks or

information systems, only through managed interfaces. Riskonnect manages the ongoing operational use of ports, protocols, and services on networked devices to minimize windows of vulnerability available to attackers.

b. Transmission Confidentiality and Integrity. Information systems protect the confidentiality and integrity of transmitted information through both physical and logical means, including employing protected distribution procedures and limiting access to peripherals (e.g., servers, computers, printers, scanners, facsimile machines), and through the use of encryption.

c. Information Protection. Riskonnect's information systems protect the confidentiality and integrity of transmitted information through both physical and logical means, including employing protected distribution procedures and limiting access to peripherals (e.g., servers, computers, printers, scanners, facsimile machines), and through the use of encryption. Any Customer Confidential Information, either at rest or in transit, will be encrypted in accordance with FIPS Publication 140-2 (FIPS PUB 140-2). Use of encryption will be compliant with all applicable export laws, rules, and regulations.

18. SYSTEM AND INFORMATION SYSTEM INTEGRITY

a. Flaw Remediation. Riskonnect: **(i)** identifies, reports, and corrects information system flaws; **(ii)** tests software and firmware updates for effectiveness and potential side effects before installation; and **(iii)** installs security-relevant software and firmware updates, including patches, service packs, hot fixes, and anti-virus signatures, once they are available. Riskonnect centrally manages the flaw remediation process, which measures the time between flaw identification and flaw remediation and establishes a process for taking corrective actions.

b. Malicious Code Protection. Riskonnect: **(i)** employs malicious code protection mechanisms at information system exit and entry points (including web browsers and email) to detect and eradicate malicious code; **(ii)** updates malicious code protection mechanisms whenever new releases are available and maintains organizational configuration management policy and procedures for managing such updates; **(iii)** configures malicious code protection mechanisms to perform periodic scans of the information systems and real-time scans of files from external sources, as the files are downloaded, opened, or executed; **(iv)** blocks, quarantines, or both, malicious code and maintains systems that send alerts to system administrator(s) in response to malicious code detection; and **(v)** addresses the receipt of false positives during malicious code detection and eradication, as well as all resulting potential impact on the availability of the information systems.

c. Information System Monitoring. Riskonnect: **(i)** monitors the information systems to detect attacks and indicators of potential attacks, and unauthorized local, network, and remote connections and identifies unauthorized use of the information system; **(ii)** deploys monitoring devices strategically within the information system and at ad hoc locations within the system; **(iii)** protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; **(iv)** heightens monitoring activity when increased risk to organizational operations, assets, individuals, other organizations, or the nation is indicated; **(v)** obtains legal opinion with regard to information system monitoring activities in accordance with applicable laws, Executive Orders, directives, policies, or regulations; and **(vi)** provides information system monitoring information to appropriate Personnel as needed.

SECURITY EXHIBIT

RISKONNECT PRODUCTS

"Platform Provider" in this Exhibit means Salesforce (force.com).

"Analytics and Data Aggregation Environment" or "ADI" in this Exhibit means Rackspace.

Standards	What we do
Regulated Data Security Controls	**Riskonnect Platform:** SSAE18 Type2, SOC2 Type2; PCI; HIPAA HITECH **Xactium Platform:** ISO27001 **ICIX Platform:** SOC2 Type2 **Riskonnect/Xactium/ICIX Platform Provider:** SSAE18 Type2, SOC2 Type2; HIPAA HITECH; PCI. Additional Platform certifications can be found at trust.salesforce.com. **Riskonnect Analytics and Data Aggregation Environment:** SSAE18 Type2, SOC2 Type2; PCI **ClearSight Platform:** SSAE18 Type2.
Patching	**Riskonnect/Xactium/ICIX Platform Provider:** Patches are remediated based on Riskonnect/Xactium Platform Provider's Patch Management Document which can be provided upon request. **Riskonnect Analytics and Data Aggregation Environment:** Riskonnect patches its infrastructure within 30 days for all patches and hot fixes following Riskonnect's change control policy. Riskonnect can apply emergency patches as necessary if the vulnerability warrants immediate remediation. **ClearSight Platform:** **Infrastructure excluding database application:** Riskonnect will patch the ClearSight infrastructure within 30 days for all patches and hotfixes following Riskonnect's change control policy. Riskonnect can apply emergency patches as necessary if the vulnerability warrants immediate remediation. **Application:**

Riskonnect will patch the ClearSight application based on the following schedule:
Critical application issue - within 14 days of identification
High - within 30 days of identification
Medium - within 60 days of identification
Low - Evaluated per major release.

Database:
Riskonnect will patch the Oracle database software within 6-8 weeks after an official Oracle PSU is released following our change control policy.

All:
Riskonnect reserves the right to apply emergency patches to any portion of our infrastructure or application as necessary to mitigate or remediate a critical vulnerability if one is identified. In all instances, Tech Ops would follow the Riskonnect change control policy.

Vulnerability Management

Riskonnect/Xactium/ICIX Platform Provider:
The Platform Provider continuously performs internal and external port scans and vulnerability scans across all of Riskonnect's environments. Any vulnerabilities would be remediated per the Patch Management Documentation.

Riskonnect Analytics and Data Aggregation Environment:
Riskonnect performs quarterly infrastructure vulnerability scans (internal and external port scans). In addition, Riskonnect engages a third party to perform an infrastructure vulnerability scan annually. Riskonnect follows the below remediation timeline:

Vulnerability Risk Rating (based on the common vulnerability scoring system)	**Remediation Timeframe**
Critical	No later than 7 days after the vulnerability is identified.
High	No later than 30 days after the vulnerability is identified.
Medium	No later than 90 days after the vulnerability is identified.
Low/Informational	As appropriate.

ClearSight Platform:

Infrastructure:
Riskonnect engages a third party to perform a quarterly external infrastructure vulnerability scan. Riskonnect follows the below remediation timeline:

Vulnerability Risk Rating (based on the common vulnerability scoring system)	**Remediation Timeframe**
Critical	No later than 7 days after the vulnerability is identified.
High	No later than 30 days after the vulnerability is identified.
Medium	No later than 90 days after the vulnerability is identified.
Low/Informational	As appropriate.

Application:
Riskonnect will patch the ClearSight application based on the following schedule:

Vulnerability Risk Rating (based on the common vulnerability scoring system)	**Remediation Timeframe**
Critical	No later than 14 days after the vulnerability is identified.
High	No later than 30 days after the vulnerability is identified.
Medium	No later than 60 days after the vulnerability is identified.
Low/Informational	Evaluated per major release.

Encryption at Rest

Riskonnect/Xactium/ICIX Platform Provider:
Platform encryption is not standard. Platform field-based encryption is available for an additional cost. Once purchased, Customer is able to manage the tenant secret used for encryption and decryption tasks.

Riskonnect Analytics and Data Aggregation Environment:

	Currently all Customer data that resides in Riskonnect's data aggregation environment is encrypted utilizing container-based encryption. All directories where Customer data is stored and encrypted using transparent data encryption. Riskonnect manages these keys. **ClearSight Platform:** All data that resides in the ClearSight platform is encrypted utilizing hardware appliance-based encryption. Riskonnect manages these keys.
Firewall	**Riskonnect/Xactium/ICIX Platform Provider:** Perimeter firewalls and edge routers are used to block unused transmission protocols, and internal firewalls are used to segregate traffic between the application and database tiers. **Riskonnect Analytics and Data Aggregation Environment:** A firewall exists in our infrastructure which allows for multi-zone network segmentation between DMZ and internal network segments. This firewall is managed by Riskonnect Technical Operations. **ClearSight Platform:** Perimeter firewalls and edge routers are used to block unused transmission protocols, and internal firewalls are used to segregate traffic between the application and database tiers.
Malware Protection	**Riskonnect/Xactium /ICIX Platform Provider:** Riskonnect's Platform Provider runs antivirus software on the production systems, which scans host filesystems (not Customer data). Definitions are updated daily. **Riskonnect Analytics and Data Aggregation Environment:** All endpoints and servers have Anti-Virus software installed and enabled. Scanning is performed in real-time. Definitions are updated daily. **ClearSight Platform:** All endpoints and servers have Anti-Virus software installed and enabled. Scanning is performed in real-time. Definitions are updated daily.
Backups	**Riskonnect/Xactium/ICIX Platform Provider:** The Riskonnect service provides real time replication to disk and near real time replication between the primary data center and the secondary data center. Backups occur over encrypted connections between servers, but are not encrypted at rest. **Riskonnect Analytics and Data Aggregation Environment:**

	Backups are done using the following schedule: Daily - Differential backup, all systems. Weekly - Full backup, all systems. Backups are stored using the following schedule: Production Systems - 4 weeks offsite. All other systems - 2 week onsite. All backups are encrypted. **ClearSight Platform:** **Database:** Backups are done using the following schedule: Block level backup - near real time replication between the primary data center and the secondary data center. **RMAN Backup:** Backups are done using the following schedule: Weekly - full backup. Daily - incremental (2-week onsite retention.**)** **OS for DB Server:** Backups are done using the following schedule: Weekly - full backup. Daily – incremental. Backups are stored onsite in the primary data center and replicated to the secondary data center. Backup is encrypted using AES256**.** **US Fileshare Backups:** Backups are done using the following schedule: Weekly - full backup. Daily – incremental. All backups replicated to the secondary data center. Backups encrypted using AES 256. **UK Fileshare Backups:** Backups are done using the following schedule: Weekly - full backup. Daily – incremental. All backups replicated to the secondary data center. Backups encrypted using AES 256.
Inventory	**Riskonnect/Xactium/ICIX Platform Provider:** Physical inventories of all production systems that reflect the current information system environment are documented and the

	inventories are maintained for tracking and reporting purposes. A physical inventory of production systems is performed periodically. **Riskonnect Analytics and Data Aggregation Environment:** All hardware and software owned by Riskonnect is entered into an Asset Inventory system inside of the Riskonnect CRM. Every asset has an owner that is entered into the asset record. **ClearSight Platform:** All hardware and software owned by Riskonnect is entered into an Asset Inventory system. Every asset has an owner that is entered into the asset record.
Credentials and Access Control	**Riskonnect/Xactium/ICIX Platform Provider:** Admin credentials and access control used by Riskonnect to provide service and support to customers are reviewed regularly by the Riskonnect Technical Operations Team. **Riskonnect Analytics and Data Aggregation Environment:** Credentials and Access Control are reviewed regularly by the Riskonnect Technical Operations Team. **ClearSight Platform:** Admin credentials and access control used by Riskonnect to provide service and support to customers are reviewed regularly by the Riskonnect Technical Operations team.
Two-Factor Authentication	Riskonnect utilizes two-factor authentication for access to all systems including access to Customer Orgs, email infrastructure, and internal systems.

Centralized Logging	**Riskonnect/Xactium/ICIX Platform Provider:** Automated, read-only audit trails are implemented and collected in the system for Customer Admins to review as needed. Logs are kept on a 6-month rolling cycle. Logs can be extracted by Customer and imported into Customer's SIEM software for further analysis as required. **Riskonnect Analytics and Data Aggregation Environment:** All log data from internal systems are collected in Riskonnect's log aggregation software. Alerts are setup for critical threshold events which can be addressed by Riskonnect Technical Operations. **ClearSight Platform:** Application logs are available to users within the platform for audit reporting purposes as required. All log data from internal systems are collected in Riskonnect's log aggregation software. Alerts are setup for critical threshold events which can be addressed by Riskonnect Technical Operations.
Intrusion Detection	**Riskonnect/Xactium/ICIX Platform Provider:** Intrusion detection system (IDS) is in place to monitor for potential security events, and the monitoring system is configured to distribute alerts as events occur. All event monitoring is done by Salesforce.com's Trust Security Organization. **Riskonnect Analytics and Data Aggregation Environment:** IDS is in place to monitor for potential security events, and the monitoring system is configured to distribute alerts as events occur. The event data is distributed to Riskonnect Technical Operations to act on and resolve. **ClearSight Platform:** IDS/WAF is in place to monitor for potential security events, and the monitoring system is configured to distribute alerts as events occur. The event data is distributed to Riskonnect Technical Operations to act on and resolve
Physical Protection	**Riskonnect/Xactium/ICIX Platform Provider:** Physical access controls, including badge readers, biometric devices, and security guards limit access to facilities and designated services areas to authorized personnel. A biometric access control system is in place at each of the data center facilities for restricted or secured areas and linked to an alarm system. Multiple two-factor authentication checkpoints are in place. Visitor policies are in place and are strictly enforced.

	Riskonnect Analytics and Data Aggregation Environment: Controlled building access and secure access to specific areas are enforced through the administration of badges/cards and biometric devices. Access to the data center is restricted through the use of biometric authentication devices and key-card-badge devices. Two-factor authentication is used to gain access to the data center and access is restricted to only authorized personnel. Visitor policies are in place and are strictly enforced. **ClearSight Platform:** Controlled building access and secure access to specific areas are enforced through the administration of badges/cards and biometric devices. Access to the data center is restricted through the use of biometric authentication devices and key-card-badge devices. Two-factor authentication is used to gain access to the data center and access is restricted to only authorized personnel. Visitor policies are in place and are strictly enforced.
Configuration Management	**Riskonnect/Xactium/ICIX Platform Provider:** An internal configuration management process that follows the Platform Provider's change control policy is in place. **Riskonnect Analytics and Data Aggregation Environment:** All changes that occur within Riskonnect's ADI environment follow Riskonnect's change control policy. The change control policy is part of Riskonnect's IS Policies and Procedures. **ClearSight Platform:** An automated tool is used to configure hardware and software used within the platform. This tool uses baseline configurations as well as iterative software manifests to consistently push patches and application upgrades across the entire infrastructure.
Incident Response Times	In the event of a confirmed security incident, Riskonnect will follow our Incident Response Plan, and customers will be notified within 48 hours of Riskonnect's knowledge of the incident.

EXHIBIT D

DATA PROCESSING ADDENDUM

This Data Processing Addendum (including its Schedules and Appendices, the "**DPA**") forms part of the Master Services Agreement between the Parties ("**Agreement**") by and between Riskonnect, Inc. and/or its Affiliates (collectively, "**Riskonnect**") and ("**Customer**"). This DPA reflects the Parties' agreement with regard to the Processing of Personal Data.

This DPA shall apply only to the services that Riskonnect provides to Customer under the Agreement ("**Services**"), notwithstanding any references in this DPA to any other services that may be offered by Riskonnect or Riskonnect's third-party software providers ("**Licensors**").

All capitalized terms not defined in this DPA have the meanings ascribed to them in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, Riskonnect and its Licensors may Process Personal Data on behalf of Customer.

DATA PROCESSING TERMS

1. DEFINITIONS

"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.

"**Customer Authorized Affiliate**" means any of Customer's Affiliate(s) which is permitted to use the Services pursuant to the Agreement between Customer and Riskonnect but has not signed their own order form with Riskonnect and is not a "Customer" as defined under the Agreement.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended (including by the California Privacy Rights Act of 2020), and its implementing regulations.

"Controller" means the entity that determines the purposes and means of the Processing of Personal Data, including, as applicable, any "business" as that term is defined by the CCPA and/or the functionally equivalent role under applicable Data Protection Laws and Regulations.

"Data Protection Laws and Regulations" means all worldwide, international, foreign, federal, state, municipal, and provincial data protection and privacy laws and regulations applicable to the Processing of Personal Data under the Agreement, including, where applicable, the GDPR, UK Data Protection Law, and the CCPA, each as amended, superseded, or replaced. For clarity, the laws of China and of Russia are expressly excluded.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"**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) and all applicable member state implementations thereof.

"Order Form" means, collectively, the Statement of Work, Project Change Order, Order, or Subscription Order as defined in the Agreement.

"Personal Data" means any information relating to a particular Data Subject.

"Processing" 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.

"**Processor**" means the entity that Processes Personal Data on behalf of the Controller, including, as applicable, any "service provider" as that term is defined by the CCPA and/or the functionally equivalent role under applicable Data Protection Laws and Regulations.

"Standard Contractual Clauses" means the applicable standard contractual clauses module(s) selected by the Parties as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and as such clauses may be subsequently updated by the European Commission, and as supplemented by the United Kingdom Information Commissioner's Office ("ICO")'s International Data Transfer Addendum to the EU Standard Contractual Clauses.

"Sub-processor" means any Processor engaged by Riskonnect related to the performance of Services under the Agreement.

"**Supervisory Authority**" means an independent public authority that is established by an EU Member State pursuant to the GDPR or the United Kingdom pursuant to the UK Data Protection Law.

"**UK Data Protection Law**" means (i) the United Kingdom General Data Protection Regulation, and (ii) the Data Protection Act 2018.

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, Customer is the Controller, and Riskonnect is the Processor. Riskonnect will engage Sub-processors pursuant to the requirements set forth in Section 5 ("**Sub-processors**") below.

2.2 Riskonnect's Processing of Personal Data. Riskonnect shall, in its provision of the Services to Customer, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations and in accordance with the Agreement, which shall be deemed as Customer's complete and final instructions with regard to the nature and purposes of the Processing.

2.3 Compliance with Law. For the avoidance of doubt, Customer's instructions to Riskonnect for the Processing of Personal Data (including those conveyed on behalf of Customer) shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data as it is entered into the Services and the means by which Customer acquired such Personal Data prior to it being entered into the Services. Customer shall not by act or omission cause Riskonnect to be in breach of Data Protection Laws and Regulations. Without limiting the generality of the foregoing, Customer represents, warrants, and covenants that that it has provided, and shall at all times throughout the term of the Agreement provide, adequate notices and has obtained and shall obtain, where required, all necessary and valid consents to provide Customer with the rights necessary to enable the lawful transfer and/or disclosure of the Personal Data by Customer to Riskonnect for the purposes set out in this Exhibit. Each Party shall notify the other Party if the Party cannot comply with applicable Data Protection Laws and Regulations in relation to this DPA. As required by applicable Data Protection Laws and Regulations, Riskonnect agrees to make available to Customer information that Riskonnect deems

reasonably necessary to demonstrate compliance with the obligations set out in this DPA and arise directly from applicable Data Protection Laws. Any such information shall be subject to the confidentiality obligations of the Agreement.

2.4 **Details of the Processing.** The subject-matter of Processing of Personal Data by Riskonnect is the performance of the Services pursuant to the Agreement. Additional Processing details, such as the duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in **Schedule 1 (Details of the Processing)** to this DPA.

2.5 **Customer Instructions.** Riskonnect shall inform Customer immediately (i) if, in its opinion, an instruction from Customer constitutes a breach of the GDPR and/or (ii) if Riskonnect is unable to follow Customer's instructions for the Processing of Personal Data.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Request.** Riskonnect shall, to the extent legally required, promptly notify Customer if Riskonnect or any of its Licensors receives a request from a Data Subject to exercise the Data Subject's rights under applicable Data Protection Laws and Regulations (each a "**Data Subject Request**"). Taking into account the nature of the Processing, Riskonnect shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Riskonnect shall upon Customer's reasonable, written request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Riskonnect 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, Customer shall be responsible for any costs arising from Riskonnect's or any of its Licensor's provision of such assistance.

4. RISKONNECT PERSONNEL

4.1 **Confidentiality.** Riskonnect shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and have received appropriate training on their responsibilities. Riskonnect shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 **Reliability.** Riskonnect shall take commercially reasonable steps to ensure the reliability of its personnel engaged in the Processing of Personal Data.

4.3 **Limitation of Access.** Riskonnect shall ensure that Riskonnect's access to Personal Data is limited to those personnel reasonably necessary for Riskonnect's performance of the Services.

5. SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Riskonnect's Affiliates and those of Riskonnect's and its Affiliates' Licensors may be retained as Sub-processors; and (b) Riskonnect and Riskonnect's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Riskonnect or a Riskonnect Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA, including any applicable Standard Contractual Clauses with

respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 **List of Current Sub-processors and Notification of New Sub-processors.** The current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Riskonnect Service, including a description of their processing activities and countries of location, can be found here: **https://riskonnect.com/legal/authorized-subprocessors**. Customer is responsible for re-checking this Sub-processor URL to obtain notice of future changes.

5.3 **Objection Right for New Sub-processors.** Riskonnect shall give Customer reasonable prior written notice, for which email or other electronic notice shall be sufficient, of the appointment of any new Sub-processor. Customer may object to Riskonnect's use of a new Sub-processor by notifying Riskonnect promptly in writing within thirty (30) days after receipt of any notice from either Riskonnect or from a Riskonnect Licensor. In the event that Customer objects to a new Sub-processor, as permitted in the preceding sentence, Riskonnect will use reasonable efforts to make available a change in the applicable Services or recommend a commercially reasonable change to Customer's configuration or use of the applicable Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Riskonnect is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided without the use of the objected-to new Sub-processor by providing written notice to Riskonnect.

5.4 **Liability.** Riskonnect shall be liable to Customer for the acts and omissions of its Sub-processors to the same extent Riskonnect would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement and subject to the mutually agreed limitations of liability, exclusion of damages, and indemnification provisions in the Agreement. Where the performance of the Services requires Riskonnect to contract with Sub-processors who only offer click-wrap data protection agreements, namely third-party cloud hosting providers, Riskonnect shall not be liable for any Sub-processors' acts of omissions that are not recoverable under the terms of such data protection agreements because of the Sub-processors' decision to impose their terms on a non-negotiable basis.

6. SECURITY

6.1 **Controls for the Protection of Customer Data.** Riskonnect shall maintain appropriate technical and organizational measures 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, Customer Data), integrity of Customer Data as it has been entered into the Services, and the confidentiality of Customer Data. Riskonnect regularly monitors compliance with these measures. Riskonnect will not materially decrease the overall security of the Services during a subscription term.

6.2 **Third-Party Certifications and Audits.** Riskonnect and its Licensors have obtained the third-party certifications and audits. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Riskonnect shall make available to Customer or to Customer's independent third-party auditor (that is not a competitor or associated with a competitor of Riskonnect) a copy of Riskonnect's and Riskonnect's Licensor's then most recent third-party audits or certifications, as applicable.

6.3 On-Site Audit. Customer may contact Riskonnect and request to conduct an audit of Riskonnect's operations and facilities ("**Audit**") to be conducted by itself or through a Third-Party Auditor (that is not a competitor or associated with a competitor of Riskonnect). An Audit may be conducted by Customer either itself or through a Third-Party Auditor (that is not a competitor or associated with a competitor of Riskonnect), selected by Customer when:

(i) the information available pursuant to section "Third-Party Certifications and Audits" is not sufficient to demonstrate compliance with the obligations set out in this DPA and its Schedules; or

(ii) Customer has received a notice from Riskonnect of a Security Incident caused by Riskonnect's breach of Applicable Data Privacy Laws & Regulations.

6.3.1 An Audit may be requested, provided that:

- Customer must provide Riskonnect with at least thirty (30) days' prior written notice requesting an Audit;
- any Audit shall be conducted at Customer's expense;
- the Parties shall mutually agree upon the scope, timing and duration of the Audit;
- the Audit shall not unreasonably impact Riskonnect's regular operations;
- any Audit does not occur more than once annually;
- any Audit restricts its findings only to data relevant to Customer;
- any Audit obligates Customer, to the extent permitted by law or regulation, to keep confidential any information gathered that, by its nature, should be confidential;
- Customer must promptly provide Riskonnect with the information regarding any non-compliance discovered during the course of the Audit; and
- Any written responses or Audit shall be subject to the confidentiality provisions of the Agreement.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

7.1 Riskonnect maintains security incident management policies and procedures. Riskonnect shall promptly notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Riskonnect or its Sub-processors of which Riskonnect becomes aware (each, a "**Data Security Incident**"). Riskonnect shall make reasonable efforts to identify the cause of such Data Security Incident and take those steps as Riskonnect deems necessary and reasonable in order to remediate the cause of such a Data Security Incident to the extent the remediation is within Riskonnect's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer, Customer Authorized Affiliates, Customer's or Customer Authorized Affiliates' third parties or agents (including Customer's third-party data providers), or any Customer Users.

8. RETURN AND DELETION OF CUSTOMER DATA

8.1 Upon Customer's written request or upon completion of the Services, Riskonnect shall return Customer Data to Customer in accordance with the terms of the Agreement and, to the extent allowed by applicable law, delete Customer Data. Until Customer Data is deleted or returned, Riskonnect shall continue to comply with this DPA.

9. CUSTOMER AUTHORIZED AFFILIATES

9.1 **Contractual Relationship.** The Parties acknowledge and agree that, by executing the Agreement including this DPA, the Customer enters into the DPA on behalf of itself. Customer agrees to the following: all access to and use of the Services and Content by Customer or by Customer Authorized Affiliate must comply with applicable terms and conditions of this DPA and the Agreement and any violation of the terms and conditions thereof by a Customer or its Customer Authorized Affiliate(s) shall be deemed a violation by Customer.

9.2 **Communication.** The Customer that is the contracting Party to the Agreement shall remain responsible for coordinating all communication with Riskonnect under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Customer Authorized Affiliate(s).

10. LIMITATION OF LIABILITY

10.1 Other than any liability that may not be limited under (i) applicable law and/or (ii) by the Standard Contractual Clauses attached hereto, each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the limitation of liability, exclusion of damages, and indemnification provisions in the Agreement, and any reference to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement and this DPA together.

10.2 For the avoidance of doubt and other than any liability that may not be limited under (i) applicable law and/or (ii) by the Standard Contractual Clauses attached hereto, Riskonnect's and its Affiliates' total liability for all claims from the Customer, or Customer Authorized Affiliates (to the extent applicable hereunder) arising out of or related to the Agreement and all DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement. Also, for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Appendices.

11. PRIVACY COMPLIANCE AND MISCELLANEOUS PROVISIONS

11.1 **Data Protection Impact Assessment.** Upon Customer's request, Riskonnect shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation(s) as a Controller to carry out a data protection impact assessment related to Customer's use of the Services by providing Customer with information published online and/or information made available to Customer through the Services. To the extent that such information made available to Customer online and through the Services is insufficient, as reasonably agreed upon by the Parties, to meet Customer's obligations under Data Protection Laws and Regulations, then Riskonnect shall provide additional reasonable cooperation and assistance to Customer necessary for completing data protection impact assessments at Riskonnect's then-current rates. Without limiting the foregoing, Riskonnect shall provide reasonable assistance to Customer in the cooperation or prior consultation with any governmental entities in the performance of its tasks relating to Section 11.1 of this DPA, to the extent required under the applicable Data Protection Laws and Regulations.

11.2 **Transfer Mechanisms for Data Transfers.** The Parties agree to enter into the Standard Contractual Clauses attached as **Schedule 2 (Standard Contractual Clauses)** hereto, as appropriate, to effectuate any transfers of Personal Data under this DPA from the European Economic Area, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data

protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations. Annex III to the Standard Contractual Clauses shall apply only with respect to transfer of Personal Data out of the United Kingdom. Riskonnect does not agree to any additions to the Standard Contractual Clauses. To the extent such terms do not contradict the terms in the Standard Contractual Clauses, the mutually agreed limitation of liability, exclusion of damages, and indemnification provisions in the Agreement and this DPA shall apply.

11.3 Supplementary Measures. The Parties agree that the following supplementary measures will apply: (a) Riskonnect: (i) has not, as of the effective date of this DPA, received any requests under Section 702 of the U.S. Foreign Intelligence Surveillance Act for the Personal Data of residents of the European Economic Area, the United Kingdom or Switzerland; and (ii) shall provide Company with notice if it receives any such request following the effective date of this DPA; (b) to the maximum extent permitted by applicable law, Riskonnect will not, to the extent legally permitted, voluntarily provide any assistance to the U.S. government in conducting operations under Executive Order 12333 with respect to Personal Data of residents of residents of the European Economic Area, the United Kingdom or Switzerland; and (c) Service Provider shall encrypt Personal Data and otherwise protect Personal Data, in each case accordance with the applicable standards set forth in Exhibit D to the Agreement.

11.4 Order of Priority. It is not the intention of either Party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses. Accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail. In no event does this DPA restrict or limit the rights of any data subject or of any Supervisory Authority. The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA shall remain in full force and effect.

12. CCPA SPECIFIC PROVISIONS

12.1 This Section 12 is only applicable to the extent Customer is subject to CCPA.

12.2 CCPA Specific Terms:

A. Definitions. The terms "**Aggregate Consumer Information**," "**Business Purpose**," "**Consumer**," "**Deidentified**," "**Personal Information**," "**Process**" (and its derivatives), "**Sell**" or "**Share**" (and their derivatives), and "**Service Provider**" shall have the meanings ascribed to them in the CCPA.

B. Customer Obligations. Customer shall comply with applicable CCPA requirements when Processing Personal Information, including but not limited to ensuring that proper notices have been provided to Consumers (i) at or prior to collection, (ii) in Customer's privacy policy, (iii) in Customer's notice of right to opt-out of Sale or Sharing, and (iv) in Customer's notice of any financial incentive for the collection of Personal Information.

C. Riskonnect Restrictions on Processing Personal Data. Customer may provide Personal Information to Riskonnect for the necessary Business Purpose of providing the offerings specified in the Agreement in its capacity as a Service Provider. Riskonnect shall not Sell or Share any Personal Information. Except as otherwise by permitted by law, including permitted internal uses of Personal Information by Service Providers under the CCPA, Riskonnect is prohibited: (a) from retaining, using, or disclosing Personal Information for any purpose other than for the specific purpose of providing the offerings specified in the Agreement and/or outside of its direct business

relationship with Customer, including retaining, using, or disclosing the Personal Information for a commercial purpose other than providing such offerings; (b) further collecting, selling, or using Personal Information except as necessary to providing such offerings; or (c) combining Personal Information Processed under this DPA with Personal Information received on behalf of other customers. The restrictions in this Section 12(C) shall not limit Riskonnect's ability to retain, use, disclose, or sell any anonymous data, Aggregate Consumer Information, or Personal Information that has been Deidentified.

D. Disclosures to Third Parties. Customer acknowledges that Riskonnect will receive and share Personal Information with its third-party partners and service providers, including but not limited to Riskonnect Licensors, in order to provide the offerings as set forth in the Agreement. Riskonnect shall enter into a written agreement with such parties, which contain obligations that are at least as protective as the terms in this Section 12. In the event that Riskonnect becomes legally compelled (by depositions, interrogatory, subpoena, civil investigative demand, similar process or otherwise) to disclose any Personal Information, Riskonnect shall provide Customer with prompt prior written notice of such requirement so that Customer may seek a protective order or other appropriate remedy.

E. Assistance with Consumer Requests. Riskonnect shall assist as may be reasonably requested by Customer to meet its obligations under the CCPA, including its obligations to respond to individuals' requests to exercise their rights thereunder. If Riskonnect receives a Consumer request directly from any Consumer whose information is Processed by Riskonnect pursuant to the Agreement, Riskonnect shall promptly provide such request to Customer and Customer shall be responsible for responding to the same.

F. Non-Exclusive Agreement/Business Associate Agreement. The rights and obligations of the Parties set forth in this Section are in addition to any additional or supplemental agreements with respect to the protection of Personal Information that may be agreed between the Parties. In the event that any offering under the Agreement requires Customer to disclose to or provide Riskonnect with access to any Protected Health Information in order for Riskonnect to fulfill its obligations under the Agreement, the Parties acknowledge and agree that this Protect Health Information is exempted from the CCPA, and the Business Associate Agreement shall exclusively govern Riskonnect's use and disclosure of such information.

List of Schedules

Schedule 1: Details of the Processing

Schedule 2: Standard Contractual Clauses

SCHEDULE 1 – DETAILS OF THE PROCESSING

Subject matter and duration of the Processing of Personal Data

The subject matter and duration of the Processing of Customer's Personal Data are set out in the Agreement and this DPA. Subject to Section 9 of this DPA, Riskonnect will process Customer's Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

The nature and purpose of the Processing of Personal Data

Riskonnect will process Customer's Personal Data as necessary to perform the Services and as may be further instructed by Customer in writing in accordance with the terms of the Agreement.

The categories of Data Subject to whom the Personal Data relates

Customer may submit Customer's Personal Data to the Riskonnect Service and other services, the extent of which is determined and controlled by Customer in Customer's sole discretion, and such Personal Data may include the following categories of Data Subjects:

- Customer Employees
- Customer's customers
- Customer independent contractors
- Customer advisors
- Customer customers' employees
- Customer's business partner employees
- Customer's vendor employees
- Customer customers' employees
- Other Users

The categories of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion.

Such Personal Data may include the following categories of Personal Data:

- Personal Name
- Title
- Business contact information (company name, email address, telephone number, physical business address)
- Personal contact information (email address, phone number, physical address)
- Employer
- Demographic information such as age and gender
- Identification number (e.g., user ID, employee ID, driver's license number, tax ID)
- Username
- Social Security number
- Account number (e.g., policy number)
- Claim data
- Policy data
- Other

Where Customer has obtained express consent from a Data Subject, Customer may additionally include the following categories of Special Category Personal Data:

- Details of any criminal records checks and associated results
- Relevant medical information (personal health information related to an insurance claim)
- Information relevant to any investigations relating to relevant employees

SCHEDULE 2 - STANDARD CONTRACTUAL CLAUSES

In the event Customer is exporting Personal Data in a manner that requires Module 2 of the Standard Contractual Clauses, the following terms will apply:

The body text of Module 2 (Controller to Processor) of the Standard Contractual Clauses attached to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 are hereby incorporated by reference. Optional aspects are described below:

1. *Clause 7 (docking clause) is omitted.*
2. *For Clause 9, Option 2: General Written Authorization is chosen.*
3. *For Clause 11, the optional text is omitted.*
4. *For Clause 17, Option 1 is chosen, with the member state being the one agreed to in the Agreement.*
5. *For Clause 18, the choice of forum is the one agreed to in the Agreement.*

In the event Riskonnect is exporting Personal Data in a manner that requires Module 4 of the Standard Contractual Clauses, the following terms will apply:

The body text of Module 4 (Processor to Controller) of the Standard Contractual Clauses attached to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 are hereby incorporated by reference. Optional aspects are described below:

1. *Clause 7 (docking clause) is omitted.*
2. *For Clause 17, Option 1 is chosen, with the member state being the Netherlands.*
3. *For Clause 18, the choice of forum is the Netherlands.*

ANNEX I

A. LIST OF PARTIES

Data exporter(s): TO BE COMPLETED BY CUSTOMER

Name: As detailed in underlying Agreement

Address: As detailed in the underlying Agreement

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Providing Personal Data to Data Importer in order for the Data Importer to Process the Personal Data as necessary to provide the Services.

Role (controller/processor): Controller

Data importer(s):

Name: Riskonnect Inc.

Address: 380 Interstate North Parkway SE, Suite 400, Atlanta, Georgia 30339

Contact person's name, position and contact details: General Counsel; privacy@riskonnect.com

Activities relevant to the data transferred under the Clauses: Processing Personal Data provided by Data Exporter in order for Data Importer to provide the Services.

Role (controller/processor): Processor

B. DESCRIPTION OF THE TRANSFER

Categories of data subjects whose personal data is transferred

As set forth in Schedule 1 to the DPA.

Categories of personal data transferred

As set forth in Schedule 1 to the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As set forth in Schedule 1 to the DPA.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The frequency of the transfer of data shall be in accordance with any applicable Subscription Order and/or Statement of Work executed by the Parties.

Nature of the processing

As set forth in Schedule 1 to the DPA.

Purpose(s) of the data transfer and further processing

As set forth in Schedule 1 to the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As set forth in Schedule 1 to the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

As determined by the Agreement.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

As set forth in the Security Exhibit attached to the Agreement.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

As set forth in the Security Exhibit attached to the Agreement.

ANNEX III – UNITED KINGDOM ADDENDUM

This Annex III hereby incorporates by reference the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force 21 March 2022, and shall be considered executed in full by all Parties to the Agreement, covering all applicable transfers under the DPA, and including all Part 2 Mandatory Clauses.