PLATFORM TERMS OF SERVICE

Carbon Signal is a registered trademark of AEDA Tools, Inc. These **Platform Terms of Service** (the "***Agreement***") are effective as of 09/10/2023 (the "***Effective Date***") and are made and entered into by and between the entity identified as the Customer (collectively, "***Customer***"), and AEDA Tools, Inc. with an address of 1450 Broadway, Suite 15-102, New York, NY 10018 ("***AEDA Tools***"). Customer and AEDA Tools collectively known as "Parties" or singularly as "Party".

WHEREAS, AEDA Tools provides certain software services. Customer desires to obtain such services from AEDA Tools, and AEDA Tools is willing to provide the same to Customer pursuant to the following terms and conditions in this Agreement. This Agreement governs the rights and obligations of the Parties pursuant to the Services provided as defined below. The Parties, therefore, agree as follows:

1. DEFINITIONS.

1.1 "***Affiliate***" means any entity now in existence or that comes into existence that directly or indirectly Controls, is Controlled by or is under common Control with Customer.

1.2 "***Confidential Information***" means non-public information that each party obtains from the other party or on its behalf in anticipation of or in connection with this Agreement relating to the disclosing party's business that the disclosing party designates as being confidential or proprietary or which, under the circumstances surrounding disclosure, is of a type that is generally treated as confidential or proprietary. Confidential Information includes, without limitation, current and prospective marketing models, plans or strategies, vendor/supplier lists, customer or consumer lists or information, Customer Data, Personal Information, former or current employee lists or information, passwords and security practices and procedures, advertising and pricing plans or strategies, databases, and data processing methodologies, algorithms, margins and expense levels, distribution and reseller arrangements, strategies and plans for the development and implementation of future products and services, refinements and additions to current products or services, trade secrets, any other proprietary, confidential or secret aspects of the parties' business.

Information is not Confidential Information if it: (a) was already in the possession of the recipient prior to its receipt from an entity other than a party or someone acting on its behalf, as shown by the recipients books and records; (b) is, or becomes, public knowledge through no fault, act or omission of the recipient; or (c) is, or becomes, available to the recipient from a source other than the disclosing party, if such source has rightfully obtained such information without an obligation of confidentiality to the disclosing party.

1.3 "***Customer Data***" means any data, information and instructions regarding the activities of Customer's business provided to AEDA Tools by Customer.

1.4 "***Intellectual Property***" means any and all completed or in-progress patentable or non-patentable: trade secrets, service marks, logos, internet URLs, copyrights, patents, inventions, original works of authorship, ideas, designs, technology, database rights, computer programs, semi-conductor

topography rights, rights of publicity, application programming interfaces, formulas, systems, techniques, know-how, data, writings, compositions, content, documents, designs, processes, procedures, all source code or object code related to any of the foregoing, or any other item, material or works that are made, conceived, developed, acquired or otherwise obtained, in any country or jurisdiction in the world, by a Party.

1.5 "***Personal Information***" means any personally identifiable information or data concerning or relating to Customer's employees, agents, customers or other individuals that Customer has dealings with, that may be used to uniquely identify or contact such employees, agents, customers or individuals as that term, or its functional equivalent, is defined in any federal, state, local or foreign privacy laws. Personal Information includes the sub-category "Personal Sensitive Information" ("***PSI***"). PSI is Customer-designated Personal Information that requires additional control and protection, which includes: credit card numbers, debit card numbers, bank account numbers, social security numbers/social insurance numbers, passwords, security challenge information, driver's license numbers, unique biometric data and Personal Identification Codes ("PIC"). PSI also includes Personal Health Information ("PHI") and Non-Public Personal Information ("NPPI"), as such terms are defined under any applicable privacy law of the United States or any other country if applicable, including but not limited to the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the Gramm-Leach-Bliley Act ("GLB") and state privacy laws, if applicable (collectively, the "***Privacy Laws***"); and any other information that Customer may identify in writing as Personal Sensitive Information.

1.6 ***"Pre-Existing Intellectual Property"*** means any Intellectual Property rights of a party that are made, conceived, developed, acquired or otherwise obtained by that party independently from any Services, software, license, or any other service provided under this Agreement.

1.7 "***Services***" means the services provided by AEDA Tools under this Agreement and as described in more detail in an applicable SOW.

1.8 "***AEDA Tools Personnel***" means the employees, approved subcontractors and independent contractors of AEDA Tools, as well as the employees and independent contractors of AEDA Tools' subcontractors.

2. DESCRIPTION OF SERVICES.

2.1 **Statements of Work**. Under this Agreement, Customer may obtain various Services that will be more fully described in an applicable Statement of Work, purchase order, or other such agreement between the Parties (each may be referred to interchangeably as an "***SOW***"). Each SOW shall be subject to the terms and conditions of this Agreement unless the SOW expressly identifies such conflict (or inconsistency) with the Agreement and stipulates to such conflict, otherwise the terms and conditions contained in this Agreement will prevail.

Any SOW shall be provided in a form similar to ***Exhibit A***. Each SOW will state the term during which the Services will be provided. If no specific term is described, the SOW will automatically terminate upon the

completion of the Service described in such SOW.

Further, if AEDA Tools provides any type of Services or products without any applicable signed or written SOW in place, the terms of this Agreement shall still apply to any such work, services, or products provided by AEDA Tools.

2.2 **Exhibits**. AEDA Tools agrees to comply with the terms and conditions set forth in the following Exhibit attached to this Agreement that are fully incorporated by reference:

Exhibit A:	Statement of Work ("***SOW***") Sample
Exhibit B:	Service Level Agreement (the "***SLA***")
Exhibit C:	Information Security Addendum (the "***ISA***")
Exhibit D:	GDPR Addendum

2.3 **Customer Corporation - Legal Relationship**. Any of Customer Corporation's Affiliates or Subsidiaries may execute an SOW or other agreement with AEDA Tools provided that such SOW is governed by the terms and conditions of this Agreement. Customer Corporation, as the ultimate parent company of its Affiliates and subsidiaries, shall be fully responsible and liable for any acts of its Affiliates or subsidiaries (including any compliance with the rights and obligations under a specific SOW) that receive Services from AEDA Tools and execute an applicable SOW for such Services under this Agreement. Any liability of Customer and any of its Affiliates or subsidiaries shall be joint and several and joint. AEDA Tools shall bill each Affiliate or subsidiary that executes a SOW separately for the Services used and purchased by such Affiliate or subsidiary.

3. TERM AND TERMINATION.

3.1 **Term**. This Agreement shall be effective during the Term. "***Term***" means the period beginning on the Effective Date listed in the introductory paragraph above and the Term shall end when the Agreement is terminated by either Party. Each individual SOW for Services shall provide a separate term for that SOW.

3.2 **Termination for Cause.** Either Party, upon giving written notice to the other Party, may terminate this Agreement and all active SOWs if: (a) the other Party materially breaches any provision of this Agreement and fails to cure that breach within thirty (30) days after its receipt of a written notice from the non-breaching Party, or if cure requires more than thirty (30) days, cure is not commenced during the 30-day period and pursued diligently to completion; (b) the other Party materially breaches any provision of the Ownership of Intellectual Property Section of this Agreement; or (c) the other Party files a petition in bankruptcy, has had a bankruptcy petition filed against it that has not been discharged within 120 days of the filing thereof, is adjudicated as bankrupt, has a receiver, trustee or other court officer appointed for its property, takes advantage of the insolvency laws of any jurisdiction to which it is subject, makes an assignment for the benefit of creditors, is voluntarily or involuntarily dissolved, or admits in writing its inability to pay debts as they come due.

3.3 **Return of Information.** Upon the expiration or termination of this Agreement and any applicable SOWs,

AEDA Tools shall promptly return to Customer any Customer Data, Pre-Existing Intellectual Property, Confidential Information, and any other related Customer material or data as reasonably requested by Customer. Upon request of Customer, AEDA Tools shall, within ten (10) business days (or any other time period agreed upon between the parties) following the termination of this Agreement or a SOW provide Customer, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to AEDA Tools), with a final extract of the Customer Data in a format that is useable by Customer or mutually agreed upon between the Parties.

Alternatively, upon Customer's request (or if any Pre-Existing Intellectual Property cannot be delivered by AEDA Tools), then AEDA Tools may destroy or irretrievably erase all Pre-Existing Intellectual Property or any other Confidential Information in its possession, custody, or control that is stored in any storage facility or media. Customer reserves the right to require AEDA Tools to provide a signed certification or verification that all Confidential Information has been destroyed or erased.

Notwithstanding the above, AEDA Tools may retain a backup copy of any of Customer Intellectual Property or Confidential Information that has been archived pursuant to the AEDA Tools' standard backup procedures and is retained solely for a regulatory or other legal compliance purposes. Such obligation on AEDA Tools to destroy and erase all Intellectual Property or Confidential Information in its possession shall not apply to the derivatives created.

4. OWNERSHIP.

4.1 **Ownership of Intellectual Property**. All Pre-Existing Intellectual Property of a Party shall remain the sole and exclusive property of that party unless otherwise agreed upon or licensed for use in this Agreement or in an applicable SOW.

4.2 **AEDA Tools License Grant**. AEDA Tools shall remain the sole and exclusive owner of all right, title and interest to its Pre-Existing Intellectual Property, however, AEDA Tools grants to Customer a perpetual, irrevocable, worldwide, royalty-free, non-exclusive, sub-licensable right and license to use any of AEDA Tools' Pre-Existing Intellectual Property to the extent incorporated in or combined with any Deliverable, or otherwise necessary for use of the Deliverable in connection with Customer's use of the Services.

4.3 **Customer License Grant**. Customer shall remain the sole and exclusive owner of all right, title, and interest in and to its Intellectual Property. Customer grants to AEDA Tools a limited, revocable, and non-sublicensable right to use any Customer Intellectual Property solely during the Term of this Agreement and only to the extent necessary to provide the Services to Customer.

4.4 **Ownership of Customer Data**. Customer Data is the sole property of Customer. Customer shall own and retain all right, title and interest in and to all Customer Data. AEDA Tools may not use Customer Data in any way except for as permitted by or required to perform under this Agreement or SOW. AEDA Tools may for any lawful purpose use Customer Data, or derivatives thereof, if it is in "cleansed" or "de-identified" form.

5. FEES & INVOICING.

5.1 **Fees**. The fees Customer shall pay AEDA Tools are set forth in each SOW. The fees shall constitute AEDA Tools' sole and complete compensation in connection with this Agreement. The fees shall not be modified during the Term except as provided herein. Customer shall not be responsible for any other fees or expenses unless specifically authorized by Customer in advance and in writing, including authorization via SOW.

5.2 **Expenses**. All pass-through or out-of-pocket expenses for which Customer is responsible must be expressly identified in the applicable SOW, and AEDA Tools will not mark-up any expenses above the amount that AEDA Tools is charged by a third party. Customer will not be responsible for the payment or reimbursement of expenses not expressly identified as a Customer responsibility in the applicable SOW.

(a) **Travel Expenses**. If the relevant SOW provides that Customer will reimburse AEDA Tools for travel (including travel, meals and lodging) expenses, AEDA Tools will obtain Customer's prior written approval for travel and all travel will be consistent with Customer's travel instructions and policies. Customer will provide relevant travel instructions and policies prior to AEDA Tools incurring any travel expenses for which it expects reimbursement.

(b) **Receipts.** Expenses will be paid through reimbursement by Customer. AEDA Tools will submit reimbursement requests (including for Travel Expenses) to Customer monthly as part of AEDA Tools' regular invoice for Services. For each expense, AEDA Tools must submit an itemized original receipt. Customer will not reimburse AEDA Tools for expenses not documented with a proper receipt.

5.3 **Invoicing**. Unless otherwise agreed to in an applicable SOW, AEDA Tools will provide Customer with a detailed invoice and Customer will remit payment of all undisputed invoices no later than sixty (60) days from its receipt of a proper invoice. Customer may not elect to set-off any amount against any sums Customer owes to AEDA Tools. Customer will provide written notice to AEDA Tools of any disputed amount within 30 days of its receipt of an invoice. The parties agree to use commercially reasonable efforts to resolve the disputed items.

5.4 **Taxes**. AEDA Tools agrees and acknowledges that AEDA Tools shall pay all taxes owed on the monies paid pursuant to this Agreement that are not subject to immediate tax withholdings by Customer. Customer and AEDA Tools agree that in the event of a challenge by any taxing authority to allocations made, or to the tax treatment of, any of the monies paid pursuant to this Agreement, each Party shall cooperate fully with the other in support of the propriety of this Agreement. AEDA Tools further agrees and acknowledges that if any taxing authority re-characterizes any of monies paid pursuant to this Agreement as wages, AEDA Tools shall indemnify and hold harmless Customer for any and all liability and costs resulting from such re-characterization, including those for taxes, penalties, interest and other costs incurred by Customer.

6. PARTY RESPONSIBILITIES

6.1 **Cooperation**. In the performance of Services, AEDA Tools will cooperate with Customer's personnel assigned and with other consultants or contractors retained by Customer in connection with related projects that may provide information related to the Services. Customer agrees to cooperate with AEDA Tools and to have its other consultants and contractors cooperate with AEDA Tools as required for performance of the Services. If applicable, each Party will appoint a project leader (as set forth in a SOW) to be responsible for coordinating and planning for cooperation in the performance of the Services in each SOW.

6.2 **Compliance with Law**. In performing AEDA Tools' obligations under this Agreement, AEDA Tools, its personnel and subcontractors, if any, shall comply with all applicable city, county, state, provincial, federal, national and international laws, ordinances, rules and regulations for any jurisdiction applicable to AEDA Tools.

6.3 **Non-exclusivity**. Unless specifically agreed to in writing in an applicable SOW, this Agreement is nonexclusive and does not grant AEDA Tools an exclusive right to provide Customer with any kind of Services, Deliverables or products and Customer may use its own employees or other contractors to perform the same or similar services as are to be performed by AEDA Tools hereunder without any liability to AEDA Tools therefor.

6.4 **Relationship of Parties**. AEDA Tools is an independent contractor, and nothing herein creates a partnership, joint enterprise, or any form of employment relationship between the parties. Neither party has the right, power or authority to bind the other to any third party or to an in any way as the representative or agent of the other, unless otherwise expressly agreed to in writing signed by both parties.

7. MAINTENANCE AND SUPPORT.

AEDA Tools shall provide to Customer maintenance and Support with respect to the Services. AEDA Tools shall provide Support to Customer consisting of, without limitation, a toll-free number for answers to Customer's questions concerning use of the Services, assistance in solving problems encountered in Customer's use of the Services and for the reporting and correction of suspected problems (collectively, "***Support***").

8. SERVICE LEVEL AGREEMENT.

AEDA Tools shall provide the Services in accordance with the service levels set forth in each SOW or on the attached Exhibit B ("***Service Level Agreement***" or "***SLA***"). If Customer provides AEDA Tools with notice of AEDA Tools' failure to meet a provision of the SLA, then AEDA Tools shall provide Customer with an applicable adjustment to the Fees as detailed in the SOW or on Exhibit B.

9. AUDIT RIGHTS.

Not more than once per year, Customer shall have the right to audit AEDA Tools' data security program and delivery of Services by giving AEDA Tools a minimum of ten (10) business days' notice of the conduct of such audit. The purpose of such audit shall be to verify that the delivery of the Services is in compliance with this Agreement or applicable SOW. The audit may include a review of AEDA Tools': (a) delivery of the Services; (b)

backup procedures; (c) disaster recovery procedures; (d) data handling procedures; (e) storage and handling of Customer's data; (f) any and all records supporting the delivery of Services to Customer; and (h) and security procedures. Customer shall be responsible for its cost for any audit.

AEDA Tools shall engage an independent third-party auditor to perform and deliver an unqualified Statement on Standards for Attestation Engagements No. 18 ("SSAE 18"), SOC 2 Type II report ("SOC 2"), which has been put forth by the Auditing Standards Board ("ASB") of the American Institute of Certified Public Accountants ("AICPA") demonstrating SOC 2 compliance. AEDA Tools shall provide Customer with a copy of AEDA Tools' most current SOC 2 report from its external, independent auditors. Additionally, AEDA Tools agrees to correct any deficiencies noted in such SOC 2 report and to retest to confirm that such deficiencies have been corrected before the end of each calendar year.

10. DATA SECURITY & PRIVACY.

10.1 **Security of Data**. AEDA Tools shall be responsible for establishing and maintaining a data privacy and information and information security program (as set forth in ***Exhibit C – the Information Security Addendum***), including physical, technical, administrative, and organizational safeguards that will secure any Customer Data (collectively, the "***Customer Information***"). Such security obligations shall include: (a) ensuring the security of any Customer Information; (b) protection against any anticipated threats or hazards to security or integrity to the Customer Information; (c) protection against unauthorized disclosure, access to, or use thereof to the Customer Information; (d) ensuring the proper disposal of the Customer Information; and, (e) ensure that all employees, agents, and subcontractor of AEDA Tools comply with all of the foregoing and are provided with training on data security and data privacy standards on an annual basis.

10.2 **Back-up and Protection of Data and Materials**. Unless otherwise specified in an SOW, to ensure uninterrupted operation in the event of an error or disaster, AEDA Tools shall provide off-site back-up storage on a daily basis of all data and materials of any type whatsoever which are related to the Services or AEDA Tools' obligations under this Agreement or which are produced in whole or in part in connection with this Agreement.

10.3 **Reconstruction of Data**. If any Customer documents, files, data or programs are lost or destroyed due to any disaster, any act or omission of AEDA Tools, or any breach by AEDA Tools of an obligation under this Agreement, AEDA Tools shall, at its own expense, promptly use commercially reasonable efforts to reconstruct such documents, files, data or programs from the back-up materials AEDA Tools is required by this Agreement to maintain.

10.4 **Additional Data Privacy for Personal Information**. Without limiting any prohibitions or obligations regarding the treatment of Personal Information, at all times during and after the Term of this Agreement, AEDA Tools shall use, handle, collect, maintain, and safeguard all Personal Information in accordance with a privacy policy reasonably acceptable to Customer and consistent with the requirements articulated in this Agreement, United States federal, provincial, and any Privacy Laws (collectively, "***Privacy Rules***") which may be in effect during the Term of this Agreement as it concerns

the subject matter of this Agreement. AEDA Tools further acknowledges that it alone is responsible for understanding and complying with its obligations under the Privacy Rules. If the Personal Sensitive Information includes any credit card or bank card information, AEDA Tools shall be responsible for complying with all applicable information security practices promulgated by the applicable federal, provincial, state, and municipal laws, regulations, and statutes pertaining to the acquisition, handling, and disposition of all such credit card information, and also by industry associations, including, but not limited to, the applicable standards of the Payment Card Industry Data Security Standard.

10.5 **GDPR**. To the extent that AEDA Tools submits, processes, or uses any Personal Data to or from the European Economic Area ("***EEA***"), the United Kingdom, or Switzerland (collectively "***Europe***"), and if applicable to the Services in any way, then the attached GDPR Addendum (***Exhibit E***) is incorporated by reference and shall apply to the extent that Personal Information includes Personal Data as defined in the GDPR Addendum. Further, AEDA Tools agrees to comply with all European Data Protection Legislation. "***Data Protection Legislation***" shall mean all applicable laws relating to data protection and privacy including (without limitation) the EU Data Protection Directive (95/46/EC) as implemented in each jurisdiction, the EU General Data Protection Regulation (2016/679), the EU Privacy and Electronic Communications Directive 2002/58/EC as implemented in each jurisdiction, and any amending or replacement legislation from time to time.

10.6 **Business Continuity.** If applicable and requested by Customer, AEDA Tools shall provide its relevant business continuity plan to Customer for review and approval prior to signing an SOW. If AEDA Tools makes material changes to its business continuity plan after execution of the relevant SOW, AEDA Tools will immediately notify Customer and send the updated business continuity plan to Customer for review.

11. <u>INSURANCE</u>.

11.1 **General**. The AEDA Tools shall purchase and maintain insurance of a form and with companies with an A.M. Best Rating of at least A- VIII and who are authorized to do business in the state(s) in which all aspects of the Services contemplated under this Agreement are to be performed. Unless otherwise stated the required insurance shall be maintained at all times during the course of AEDA Tools' performance under this Agreement. All policy forms must provide coverage at least as broad as the current form promulgated by the Insurance Services Office ("ISO"). If no such form is available, then the policy is subject to approval by Customer. AEDA Tools is responsible for its own deductibles and retention.

11.2 **Certificate of Insurance**. Before commencement of the services, AEDA Tools shall furnish to Customer, Certificates of Insurance evidencing the following coverages. It is the responsibility of AEDA Tools to secure evidence of the same coverage from any engaged sub-contractors. AEDA Tools shall provide thirty (30) days' prior written notice in the event of any termination, non-renewal or cancellation or any material change in coverage or deductibles. This requirement does not invalidate any prohibition in this Agreement against the use of sub-contractors. General conditions applying to all insurance coverage are that: 1) no policy shall contain a self-insured retention; and 2) no policy shall contain a deductible in excess of $25,000; and 3) satisfaction of any/all deductibles shall be the sole responsibility of AEDA

Tools.

11.3 **Additional Insured**. Customer and any party reasonably requested by Customer must be included as additional insureds under AEDA Tools' commercial general liability and excess/umbrella liability policies. These policies must also provide for a waiver of subrogation of the carrier(s)' rights that is in favor of these entities. Additional insured coverage procured by AEDA Tools shall be primary and shall under no circumstances be construed to apply as excess or contribute with any insurance coverage independently carried by any of the additional insureds. The policies cannot contain any provision that would preclude coverage for suits/claims brought by an additional insured against a named insured.

11.4 **Insurance Coverage Requirements.** AEDA Tools agrees to obtain the following insurance coverages:

Type	Limits
Workers' Compensation: As required by the applicable state statute for its employees, including the following requirements: (i) AEDA Tools agrees to have its workers' compensation insurance policy amended to waive the insurer's rights of subrogation against Customer for recovery of claims paid under AEDA Tools' policy, but only for losses caused by and to the extent of AEDA Tools' negligence; and (ii) If AEDA Tools is not required by law to maintain workers' compensation insurance, AEDA Tools will maintain private health insurance for its employees (at its sole expense).	Statutory limits and contain employer's liability coverage in an amount not less than U.S. $1,000,000.00 per accident for bodily injury and disease covering all diseases.
Automobile Liability: Covering all vehicles owned, non-owned, hired and leased.	An amount not less than U.S. $1,000,000.00 per claim (combined single limit for bodily injury and property damage)
Commercial General Liability ("CGL"): Written on an occurrence basis, utilizing standard unmodified coverage forms, with per project/per location aggregate endorsements applicable to the Services contemplated under this Agreement. AEDA Tools must also carry an installation floater or fungible form of property coverage to cover loss or damage to any equipment or material to be installed in connection with the Services. Coverage insuring against bodily injury, property damage, contractors' completed operations and contractual liability (covering AEDA Tools' indemnification obligations contained in the Agreement) Coverage shall provide that any individual or entity that AEDA Tools is	a combined single limit of not less than U.S. $2,000,000.00 per claim (This limit may be obtained through combining CGL and excess/umbrella policies. The "product/completed operations" aggregate shall be no less than the general aggregate)

obligated to name as an additional insured shall automatically receive additional insured status under the CGL policy. Additional insured coverage for all liability in connection with the subject matter of this contract must extend to include product/completed operations coverage. Products/completed operations insurance shall be maintained for a minimum period of three (3) years after final payment and Service	
Professional liability and errors and omissions The coverage shall respond on a claims-made basis and shall remain in effect for a period of three (3) years after completion of all Services under this Agreement. AEDA Tools shall continue to provide evidence of such coverage to Customer on an annual basis during the aforementioned period.	an amount not less than U.S. $5,000,000.00 per claim.
Umbrella coverage (including commercial general liability coverage)	not less than U.S. $5,000,000.00 over the coverage shown above.
Privacy, Network Security and Cyber Liability Covering all networks and information.	Not less than U.S. $10,000,000.00 per claim.
Crime Insurance	Not less than $10,000,000.00 per claim.

12. CONFIDENTIALITY.

12.1 **General Requirements**. During the Term of this Agreement or applicable SOW, either Party may disclose (the "***Discloser***") or provide to the other Party (the "***Recipient***") Confidential Information in connection with the Services or in connection with this Agreement or applicable SOW.

12.2 **Use of Confidential Information**. Recipient may use Confidential Information of the Discloser only for the purposes of exercising Recipient's rights and fulfilling Recipient's obligations under this Agreement and shall not disclose or allow the disclosure of the other Party's Confidential Information to any unauthorized third party. Recipient shall use the same degree of care, but not less than a reasonable degree of care, to protect against the unauthorized disclosure or use of Discloser's Confidential Information as it uses to protect its own confidential information of a similar type. Recipient shall disclose Confidential Information of Discloser only to its employees, independent contractors, and agents who have a need to know the Confidential Information as related to the Services provided, and who are bound by obligations of confidentiality no less restrictive than the terms of this Agreement. Recipient shall not remove any confidentiality or proprietary notices from Discloser's Confidential Information.

12.3 **Exceptions**. Recipient's obligation under this Agreement to treat information as Confidential Information does not apply to information that: (i) is already known to Recipient at the time of disclosure and was not obtained, directly or indirectly, from Discloser; (ii) is independently developed by Recipient without reference to or use of the Discloser's Confidential Information; (iii) is obtained by Recipient from another source without a breach of any obligation of confidentiality owed by that source to Discloser; or (iv) is or becomes part of the public domain through no wrongful act of Recipient or any party that obtained the information from Recipient. If Recipient is served with a subpoena or other legal process, court, or governmental request or order requiring disclosure, or is otherwise required by law or securities exchange requirement to disclose, any of Discloser's Confidential Information, Recipient shall, unless prohibited by law, promptly notify Discloser of that fact and cooperate fully (at Discloser's expense) with Discloser and its legal counsel in opposing, seeking a protective order, seeking to limit, or appealing the subpoena, legal process, request, order, or requirement to the extent deemed appropriate by Discloser. Recipient may comply with the subpoena or other legal process or requirement after complying with the foregoing sentence, but only to the extent necessary for compliance. A non-public disclosure made pursuant to the foregoing sentence will not, by itself, remove any Confidential Information from the protections of this Agreement.

12.4 **Injunctive Relief**. The Parties agree that an impending or existing violation of any provision of the Confidentiality obligations in this Agreement may cause the Discloser irreparable injury for which it would have no adequate remedy at law and agree that the Discloser shall be entitled to seek immediate injunctive relief prohibiting such violation, without the necessity of posting bond, in addition to any other rights and remedies available to it.

13. WARRANTIES.

13.1 **General Mutual Warranties**. Each Party represents and warrants that: (i) it is a duly organized and validly existing corporation, and is in good standing in the laws of the state in which the respective entity was formed; (ii) it has all authorizations, approvals and consents required for the execution of this Agreement and fulfillment of its obligations herein; (iii) it has full right, power and authority to enter into this Agreement and properly carry out all of the terms hereof; (iv) at all times during the term of this Agreement, each Party shall fully comply with all applicable federal and state laws, including all employment laws and obligations as an employer.

13.2 **Intellectual Property Warranty**. AEDA Tools represents and warrants that the Services and Customer's exercise of its licenses set forth in this Agreement with respect to the Services, will not infringe, any third-party Intellectual Property right.

13.3 **Services Warranty**. AEDA Tools represents and warrants that:

(a) all Services delivered shall strictly comply with all applicable specifications, descriptions, and other conditions of this Agreement and any SOW; and
(b) all Services are in compliance with all federal, state and local laws, whether in the form of statutes, regulations, rules, standards, guidelines, judicial or administrative decisions, or any

other federal, state or local action having the effect of law; and that it will comply with all applicable laws, rules, and regulations regarding the provision of the Services.

13.4 **Limitation on Warranty**. WITH THE EXCEPTION OF EXPRESS WARRANTIES CONTAINED IN THIS AGREEMENT OR ANY SOW, SERVICE PROVIDER PROVIDES THE SERVICES AS IS, WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED, AND SERVICE PROVIDER DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

14. INDEMNIFICATION.

14.1 **AEDA Tools Indemnity.** AEDA Tools will indemnify, defend, and hold harmless Customer (including any of Customer's Affiliates, officers, directors, shareholders, employees and agents) (collectively "*Customer Indemnitees*") from and against any and all claims, suits, demands, actions, damages, judgments, fines, fees, costs, and expenses, including reasonable attorneys' fees, arising from or related to any damages or liability arising from a third-party regarding:

(a) A breach of Confidentiality or the Data Security & Privacy obligations of this Agreement; or

(b) Any allegation that the Services or any other materials or resources provided to Customer by AEDA Tools or Customer's Indemnitees' use thereof constitutes an infringement, contributory infringement or violation of any patent, copyright, trade secret, trademark, or other third-party intellectual property right (including any misappropriation of a trade secret or other personal rights of a third party).

14.2 **Intellectual Property Mitigation.** In the event of a claim relating to any Intellectual Property of any third party, in addition to and not in lieu of any obligations set forth above, AEDA Tools will have the option to: (a) secure the right for Customer to continue using the infringing service or software; (b) replace the infringing service or software with a functionally equivalent non-infringing version thereof; (c) modify the infringing service or software so it becomes non-infringing without incurring a material diminution in performance or function; or (d) in the event AEDA Tools can accomplish neither of such actions, and only in such event, AEDA Tools may terminate this Agreement and refund Customer for any fees paid with respect to such infringing item provided by AEDA Tools, on a pro-rated basis taking into account the amount of time that was paid for but which was not used by Customer.

14.3 **Customer Indemnity.** Customer will indemnify, defend, and hold harmless AEDA Tools (including any of AEDA Tools' Affiliates, officers, directors, shareholders, employees and agents from and against any and all claims, suits, demands, actions, damages, judgments, fines, fees, costs, and expenses, including reasonable attorneys' fees, arising from or related to any damages or liability arising from a third-party regarding:

(a) Customer Data;

(b) An allegation that a Customer service or product directly infringes any third-party's registered patent or copyright, or misappropriates any trade secret;

(c) Customer's gross negligence, willful misconduct, or fraudulent conduct; and

(d) Any personal injury (including death) or damage to property resulting from Customer's acts or

omissions.

14.4 **Notice**. The indemnifying party's obligations under this Section are conditioned upon the indemnified party providing the indemnifying party with: (1) prompt written notice of the existence of the claim, suit, action or proceeding giving rise to the potential indemnification obligation hereunder (each a "***Claim***"); (2) authority, at the Indemnitee's option, for sole control over the defense or settlement of such Claim, provided that neither Party shall settle such Claim without the other Party's prior written consent, which consent shall not be unreasonably withheld, conditioned or delayed; and (3) assistance at the indemnifying party's request and expense to the extent reasonably necessary for the defense of such Claim.

15. LIMITATIONS OF LIABILITY AND WARRANTIES.

15.1 **Liability Cap.** THE AGGREGATE LIABILITY OF EITHER PARTY, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, IN CONNECTION WITH ANY OF THE SERVICES PROVIDED PURSUANT TO A SOW UNDER THIS AGREEMENT, SHALL IN NO EVENT EXCEED THE AMOUNT PAID OR PAYABLE TO SERVICE PROVIDER FOR SERVICES UNDER THIS AGREEMENT.

15.2 **No Indirect Damages**. NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR OTHER ECONOMIC LOSS ARISING UNDER THIS AGREEMENT. THIS LIMITATION OF LIABILITY WILL APPLY REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT OR TORT, INCLUDING NEGLIGENCE AND INDEPENDENT OF ANY FAILURE OF ESSENTIAL PURPOSE OF THE REMEDIES PROVIDED HEREUNDER, AND SHALL APPLY WHETHER OR NOT A PARTY HAS BEEN APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

16. DISPUTE RESOLUTION.

16.1 **Disputes and Venue**. Any action relating to or in connection with this Agreement or any SOW shall be brought and maintained exclusively in any state or federal court, in each case located in Fulton County, Georgia. Each Party to this Agreement or any SOW hereby expressly and irrevocably submits to the jurisdiction of such courts for the purposes of any such action and expressly and irrevocably waive, to the fullest extent permitted by law, any objection which it may have or hereafter may have to the laying of venue of any such action brought in any such court and any claim that any such action has been brought in an inconvenient forum.

16.2 **Choice of Law***.* This Agreement shall be interpreted under the laws of the State of Georgia, without regard to that body of law controlling conflicts of law. In any suit or proceeding to enforce rights under this Agreement, the prevailing Party shall be entitled to recover costs and attorneys' fees.

16.3 **Remedies not Exclusive***.* Unless this Agreement expressly states that a remedy is exclusive, no remedy made available under this Agreement is intended to be exclusive.

17. MISCELLANEOUS PROVISIONS.

17.1 **Assignment**. Customer may not assign any right under this Agreement without the prior written consent of AEDA Tools, which consent may be granted or withheld by AEDA Tools in its reasonable and sole discretion but shall not be unreasonably withheld. Any such attempted assignment without such prior consent shall be wholly void.

17.2 **Publicity**. AEDA Tools may refer to Customer (or any of its Affiliates) or use Customer's logos or other trademarks in any manner, in any news release, advertising, solicitations or disclosure of a similar nature as part of its marketing efforts.

17.3 **Force Majeure**. No Party shall be responsible for any loss or damage to the other Party if that Party is unable to fulfill any part of its obligations under this Agreement, or is prevented or delayed from fulfilling such obligation, due to flood, fire, earthquake or other acts of God, war or hostilities, invasion, rebellion, riot, strike, lockout, court order, epidemic, pandemic (including the pandemic caused by the novel coronavirus that causes COVID-19) or any other cause beyond the control of the Party ("***Force Majeure***"). If a Force Majeure occurs, the Party affected shall promptly notify the other Party. The rights and obligations of a Party shall be suspended only for the duration and extend of the Force Majeure and once the Force Majeure ceases to exist, the rights and obligations of the parties shall continue in full force and effect.

17.4 **Notices**. All notices and other communications hereunder will be in writing and will be deemed to have been given (a) when personally delivered, or (b) five (5) business days after being mailed by first class U.S. mail, return receipt requested, or (c) when delivered by other electronic transmission device, delivered as specified hereafter for each Party (unless a substitute address is specified in writing):

Notices to Customer:

With a Copy to:

Notices to AEDA Tools:

Attn: Shreshth Nagpal
AEDA Tools Inc.
1450 Broadway Suite 15-102
New York, NY, 10018
Email: shreshth@carbonsignal.com

17.5 **No Waiver**. No delay or omission by either Party in exercising any right or remedy hereunder available to that Party shall operate as a waiver of such right or remedy or any other right or remedy. No waiver of any right, obligation or default shall be effective unless it is in writing and signed by the Party against whom the waiver is sought to be enforced. One or more waivers of any right, obligation or default shall

not be construed as a waiver of any subsequent right, obligation or default.

17.6 **Severability**. Any provision or provisions of this Agreement which shall prove to be invalid, void or illegal shall in no way affect, impair or invalidate any of the other provisions, and shall be modified or excised to the minimum extent possible so that this Agreement otherwise remains enforceable and in full force and effect. No ambiguity herein shall be construed against either Party as the drafter, as each Party has reviewed this Agreement with its counsel.

17.7 **Survival**. The following Sections in this Agreement with the following headings shall survive termination of this Agreement: Confidentiality, Limitation of Liability, Indemnification, Audit Rights, Intellectual Property Right, Data Security and Privacy, Warranties, Insurance, Dispute Resolution, and Miscellaneous.

17.8 **Entire Agreement**. This Agreement, any Statements of Work, Exhibits and any mutually-executed amendments or attachments thereto and any materials incorporated herein by reference, represent the complete and entire agreement between the parties regarding the subject matter hereof, and supersedes all prior agreements and understandings between the parties. This Agreement may not be amended except through a writing signed by each of the parties hereto.

17.9 **Counterparts**. This Agreement may be executed in counterparts, all of which when executed and delivered, shall constitute one single agreement between the parties.

THE PARTIES EVIDENCE THEIR AGREEMENT WITH THE ABOVE TERMS AND CONDITIONS BY SIGNING BELOW.

CUSTOMER	**AEDA TOOLS**
By: _____	By: _____
Name:_____	Name:_____
Title: _____	Title: _____
Date:_____	Date:_____

EXHIBIT A

SAMPLE Statement of Work

Instructions: The following is a sample SOW that the Parties may elect to use as a template when Customer purchases Services from AEDA Tools. The form and substance may change as agreed upon between the Parties.

Sample Statement of Work:

This Statement of Work and its attachments (if any) are, by this reference, subject to the terms of and made a part of the Master Services Agreement ("Agreement") dated _____ by and between [ENTER NAME OF CUSTOMER ENTITY PAYING SERVICE PROVIDER] ("Customer") with an address of 3680 Victoria Street N., Shoreview, MN 55126, and [insert AEDA Tools name] ("AEDA Tools") whose business address is _____. Capitalized terms used but not defined in this SOW shall have the meanings given to them in the Agreement.

1. **GENERAL PURPOSE & SUMMARY OF SERVICES:**

   Under this SOW, AEDA Tools is licensing its INSERT PRODUCT NAME (the "Services") to Customer so that it may use the Services for [INSERT BUSINESS PURPOSE here] [and, if applicable: as a part of a Combine Solution].

2. **TERM:**

   This SOW is effective as of ***X*** ("Effective Date") until ***X*** ("End Date") unless otherwise terminated pursuant to the Agreement.

3. **DESCRIPTION OF SERVICES:**

   [This should be the details of "what" and "how" the Services are being provided....]

   (a) **General Description**

   AEDA Tools will provide [INSERT GENERAL DESCRIPTION].

   (b) **Phase I or Service Features**

   INSERT, if applicable, the general phases of what will be delivered and how it will be delivered, or give specific and material facts about how the Deliverables are provided.

4. **PROJECT LEADERS:**

   The following individuals shall be defined as the Project Leaders of Customer's project:

AEDA Tools Project Leader(s)	**Customer Project Leader(s)**

• Name • Name	• Name • Name

5. **DELIVERABLES:**

As the final output and result of the Services, AEDA Tools will provide the following Deliverables to Customer:

- XXX

6. **FEES/COSTS & INVOICING:**

[INSERT]

Invoicing:
AEDA Tools shall invoice Customer [on a monthly basis/annual basis or _____]

Customer shall pay all undisputed amounts within forty-five (45) days of the invoice date. Invoices shall be submitted to: payables@XXXXXXX.com

Applicable federal, state, and local taxes are not included in the total amount due.

7. **ENTIRE AGREEMENT:**

The terms and conditions in this SOW is the Parties' complete understanding and agreement of the Services provided. In the event of a conflict between this SOW and the Agreement, the Agreement will control unless otherwise agreed upon between the parties in this SOW. No other terms and conditions, beyond those contained therein, will be valid unless mutually agreed upon in writing, and signed by a representative of each Party.

IN WITNESS WHEREOF, Customer and AEDA Tools have caused this Agreement to be executed as of the date first above written by their respective officers thereunto duly authorized.

AEDA TOOLS	**CUSTOMER**
EXAMPLE ONLY	EXAMPLE ONLY
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

Date:		Date:	

EXHIBIT B

Sample Service Level Agreement

This Service Level Agreement ("SLA") and its attachments (if any) are, by this reference, subject to the terms of and made a part of the Agreement. Capitalized terms used but not defined in this SOW shall have the meanings given to them in the Agreement.

1. **SEVERITY LEVELS**. The following severity levels define the level of importance and effort necessary by AEDA Tools to remedy each issue that is reported to AEDA Tools' help desk.

1.1 **Severity Level 1.** Severity Level 1 are issues that cause Services to cease functioning. There is no way to work around the problem and Customer cannot function in its daily business. AEDA Tools will respond within fifteen (15) minutes of being notified either through system monitoring or Customer notification**.** The response will include providing Customer with information regarding the nature, scope, expected duration and plan of action to resolve the incident. The response may include notice by email message, telephone call, text message, or other means, which may or may not provide for proof of delivery. AEDA Tools will immediately and continuously work until a resolution suitable to Customer is found and placed into productive use. Time is of the essence. AEDA Tools will correct the problem or install an effective work around within eight (8) hours of receiving notice from Customer of the problem.

1.2 **Severity Level 2.** Severity Level 2 issues severely restrict Customer's ability to use the Services. The Services may be functioning, but at a level that does not allow normal daily responsibilities to be completed. AEDA Tools will respond within thirty (30) minutes**.** AEDA Tools will immediately and continuously work until a resolution suitable to Customer is found and placed into productive use. Time is of the essence. AEDA Tools will correct the problem or install an effective work around within twenty-four (24) hours of receiving notice from Customer of the problem.

1.3 **Severity Level 3.** Severity Level 3 issues have an impact on daily operations. Customer is unable to utilize certain capabilities within the Services and Materials. AEDA Tools will respond within two (2) hours of receiving notice from Customer of the problem. AEDA Tools will provide a fix or workaround suitable to Customer within five (5) business days.

1.4 **Severity Level 4.** Severity Level 4 issues are "nice to have" modifications to the system that have no impact on the daily operations. AEDA Tools will work with Customer to enhance the capabilities of the system throughout the Term of the Agreement.

2. **NOTICE**. Customer shall be promptly notified following the discovery of any condition(s) (including, but not limited to those listed below) that present the potential for a Severity Level 1 or Severity Level 2 issue. These conditions include:

- hardware or operating system instability that may cause the system to become inaccessible or damage any data.
- network instability that may cause the system to become inaccessible or damage any data.

- the presence of a virus.
- detection of unauthorized user access or other hacking into the network.

For each issue reported to AEDA Tools by Customer that is a Severity Level 1 or Severity Level 2 issue and AEDA Tools fails to remedy such issue in the times set forth above with respect to such Severity Levels 1 or 2 as applicable, AEDA Tools shall credit Customer's next month's invoice with a five percent (5%) credit for each and every period for the specific severity level on all affected service(s); e.g. if there is a Severity Level 1 issue that has Customer business unit unable to work, for every calendar eight hours that the Severity Level 1 problem is not fixed, AEDA Tools will credit Customer five percent (5%) of the next month's invoice. For each issue reported to AEDA Tools by Customer that is a Severity Level 3 issue and AEDA Tools fails to remedy the issue in the times listed above, AEDA Tools shall credit Customer's next month's invoice with a two percent (2%) credit on all affected services.

These Service Levels shall be measured using a monthly report, provided by AEDA Tools, that documents time and nature of calls (or preferred method of notice) to the Customer's service team, time and date of initial response, and time of problem resolution. Resolution is defined as the case being closed by Customer.

If AEDA Tools fails to fix a Severity Level 1 or Severity Level 2 issue in the allotted timeframe four (4) or more times in a rolling three (3) month period, Customer shall have the right to immediately terminate this Agreement for Cause as described in the Agreement.

3. AVAILABILITY, DOWNTIME AND RESPONSE TIME DEFINITIONS

a. "***Available***" shall mean the Service or system is up, running and responsive to ping requests and is providing Customer the functionality and the Services described in an Exhibit and any SOW.

b. "***Availability***" shall be 99.99% Available and shall mean Scheduled Uptime minus Unplanned Downtime, divided by Scheduled Uptime multiplied by 100 (to determine a percentage). For purposes of determining whether AEDA Tools' performance meets any Service Level, AEDA Tools' performance will be measured based on a monthly average for the Services and Materials.

c. The following is 'Availability' expressed as a mathematical formula:
   i. A = Availability
   ii. UD = Unplanned Downtime
   iii. SU = Scheduled Uptime
   iv. ED = Excusable Downtime
   v. A = [(SU - (UD - ED)/SU] x 100

d. The following is an example, determined on a monthly basis, using the above formula:
   i. SU = 720
   ii. UD = 9.5 hours
   iii. ED = 3

iv. [(720 - (9.5 - 3)/720] x 100 = 99.09%.

e. "***Scheduled Uptime***" shall mean the days of the week and hours per day that the Services and Materials or network is scheduled to be Available for use by Customer subject to Scheduled Downtime.

f. "***Scheduled Downtime***" shall mean, of the Scheduled Uptime, the aggregate number of hours in any calendar month during which the system or network is scheduled to be unavailable for use by Customer due to such things as preventive maintenance, system upgrades, etc.

g. "***Unplanned Downtime***" shall mean, of the Scheduled Uptime, the aggregate number of hours in any calendar month during which the system or network is unavailable.

h. "***Excusable Downtime***" shall mean, of the Scheduled Uptime, the aggregate amount of time in any calendar month during which the Services and Materials or network is unavailable for use by Customer due to action or inaction by Customer, its vendors or agents, or due to a force majeure event, which is excusable under this Agreement. Emergency system maintenance shall be considered Excusable Downtime.

i. "***Response Time***" shall mean the amount of time that elapses between the time a Customer authorized user of the system hits the enter button on a keyboard to the time that the system response is displayed on such authorized user's screen. Response Time shall not exceed one (1) second.

It may be necessary to temporarily restrict access to Customer's application(s) and/or database(s) without prior notice to protect the integrity of the application and database; such restricted access shall be considered Excusable Downtime for the purpose of calculating Service Levels.

For each month that the system Availability is ***less than 99.95% or the average Response Time is greater than one second***, AEDA Tools shall credit Customer's next month's invoice with a five percent (5%) credit for the total monthly fees. If this system Availability and Response Time service level is not met for three (3) consecutive months, Customer shall have the right to immediately terminate this Agreement for cause as described in the Agreement.

EXHIBIT C

Information Security Addendum

This Information Security Addendum (the "***ISA***") is intended to detail AEDA Tools' obligations under applicable law and the Agreement and is made part thereof. In case of any conflict between the MSA and this ISA, the terms and conditions of this ISA shall control. Capitalized terms used, but not defined, herein shall have the meaning ascribed to them in the MSA.

1. GENERAL ACKNOWLEDGEMENT OF OBLIGATIONS.

AEDA Tools understands that the requirements set forth in this ISA are intended to detail AEDA Tools' obligations under applicable law and the MSA, and that these requirements are not intended to be comprehensive statements of how AEDA Tools should implement or meet such requirements. Where local laws and regulations require controls that are more restrictive than, or in conflict with, those identified in this ISA, AEDA Tools shall comply with those control requirements. Customer's audit rights set forth in the MSA shall remain unaffected by AEDA Tools' compliance with the requirements set forth in this ISA. This ISA shall not create any additional rights for AEDA Tools, nor shall it impose liability on Customer or its Affiliates. Unless otherwise provided in a SOW or other writing signed by both parties, AEDA Tools shall be responsible for all costs of compliance with the terms of this ISA. A breach of the requirements set forth in this ISA shall be deemed a breach of the MSA, and Customer shall have all rights accorded to it as set forth in the MSA.

2. SERVICE PROVIDER REQUIREMENTS.

AEDA Tools shall comply with the following information security requirements:

2.1. Audit Rights and Administration. AEDA Tools shall provide assurance that the appropriate level of information security is present and maintained while AEDA Tools is providing Services or accessing, processing, or using any Customer Data. AEDA Tools shall comply with the following:

(a) Upon Customer's request, providing any of the following within thirty (30) days of the request: (i) a completed Customer risk assessment questionnaire (as provided by Customer); any third-party audit reports of AEDA Tools' information security program (i.e., SOC, PCI AOC, ISO certificate or other similar reporting); (ii) a summary of assessments and/or tests completed on AEDA Tools' third parties that access Customer Data or systems; (iii) a network diagram; (iv) a data-flow diagram; (v) a summary of AEDA Tools' information security protocols; physical access control management documentation, background screening overview; (vi) a copy of AEDA Tools' code of conduct; (vii) Business continuity plans and summary; (viii) AEDA Tools' disaster recovery plans; and (ix) any applicable insurance certificates (with submission of requested supporting artifacts – including policies and procedures, if applicable).

(b) If appropriate and upon Customer's request, AEDA Tools will participate in security awareness training activities.

(c) Any ad hoc requests by Customer to fulfill due diligence for: (i) changes in applicable laws or regulations that require compliance, including, but not limited to instances where AEDA Tools incurs material changes relevant to the Services (i.e., significant network and/or system changes, acquisitions or divestitures, etc.); (ii) Customer requests due to requirements under new

Customer client agreements; or (iii) instances where AEDA Tools incurred an information Security Breach.

(d) Any concerns identified by Customer with AEDA Tools' responses to Customer's information security requests shall be discussed and evaluated as necessary.

2.2. Remediation. AEDA Tools agrees that any remediation items reasonably identified as a result of Customer's assessment must be resolved as soon as possible on a timetable commensurate with the risk, and AEDA Tools must provide evidence of remediation.

2.3. Security Breaches.

(a) Notification. AEDA Tools shall notify Customer after the confirmation of any Security Breach involving Customer Data within twenty-four (24) hours of its discovery. A "***Security Breach***" means any intentional or unintentional misuse, unauthorized destruction, loss, availability, alteration of or access to any Customer Data, or any breach or suspected breach of the safety and security procedures in this ISA.

(b) Investigation and Cooperation. AEDA Tools shall immediately undertake all reasonable efforts to investigate, correct and remediate any Security Breach in a manner that meets or exceeds industry standards, including cooperating with any governmental or other investigative entity with jurisdiction for the Security Breach. AEDA Tools shall cooperate and maintain timely communications with Customer during its investigation of the Security Breach. AEDA Tools will not inform any third party of Customer's involvement in any such Security Breach without Customer's prior written consent (excluding AEDA Tools' legal advisors, insurance carrier, those parties engaged to assist in resolving the Security Breach, or as may be strictly required by applicable law). If AEDA Tools' disclosure is required by applicable law, AEDA Tools agrees to work with Customer prior to any disclosure regarding the content of such disclosure so as to minimize any potential adverse impact upon Customer and its clients and customers. Notwithstanding anything to the contrary set forth in this Agreement, all costs associated with any Security Breach, including but not limited to, the costs of notices to and at least two (2) years of credit monitoring for any affected persons shall be the sole responsibility of AEDA Tools. The remedies and obligations set forth in this subsection are in addition to any others Customer may have.

(c) Security Breach Management Program. AEDA Tools shall establish a program to respond appropriately in to a suspected or detected Security Breach that may result in the loss or unauthorized access of Customer Data. In responding to any Security Breach, AEDA Tools shall have established and written controls, processes or procedures in place that shall include, but not be limited, to the following: (i) Reporting Security Breaches or other security-related incidents by anyone having access to AEDA Tools' information security environment; (ii) Evidence recovery and preservation; (iii) Third-party (including law enforcement and regulators) coordination and communication; (iv) Formal defined roles and responsibilities; (v) Established priority levels of

incident types; (vi) Defined communication plans to ensure participation in Security Breach resolution and management awareness; and (vii) Having all Security Breach monitoring controls implemented on configurable systems and devices transmitting or housing: applications, databases, servers, networking gear, and on any security system or critical system that processes Customer Data.

(d) Logging. AEDA Tools' applications and databases shall provide logging for Security Breaches (including suspected Security Breaches) that can only be detected within the application or database. Security Breach log thresholds shall be defined to facilitate effective log reviewing processes (including suspected Security Breaches).

(e) Documentation. Security Breaches (including suspected Security Breaches) shall be documented and the following shall be included in the log: (i) Event type; (ii) Time stamp and address information associated with the originating device (such as terminal ID, port number, network address and/or device name); (iii) System or information resource accessed in the event; (iv) Result of event; and (v) Reason for failure, relative to information protection requirements, as applicable to security event types resulting in failure.

(f) Security Breach/Security Event Recovery. AEDA Tools shall have documented procedures for incident containment and recovery. Automatic alerts shall notify AEDA Tools to identify high-risk and other security-related events.

2.4. Information Security Requirements. AEDA Tools will abide by the following information security guidelines by implementing the below "Control Activities":

Control Objective	Control Activity	Risk Statement
Policies for Information Security	AEDA Tools must define, approve, publish and communicate an information security policy. AEDA Tools must review, update, and approve policies on an annual basis. Policies must be communicated to all employees and appropriate external contacts.	Without security policies in place, AEDA Tools will not apply defined protection measures to secure data and resources.

Control Objective	Control Activity	Risk Statement
Information Security Roles and Responsibilities	AEDA Tools must have information/cyber risk governance processes in place that ensure an understanding of AEDA Tools' technology environment and the state of information/cyber security controls, and a security program to protect AEDA Tools from information/cyber threats in accordance with good industry practice (including NIST, SANS, ISO27001) and applicable industry requirements. AEDA Tools shall undertake regular risk assessments in relation to information/cyber security (and, in any event, not less than once every twelve (12) months) and shall implement such controls and take such steps as are required to mitigate the risks identified. AEDA Tools must maintain senior management-approved policies, and standards to manage Customer's information/cyber risk, and must review these at least annually.	Without appropriate information security roles and responsibilities, AEDA Tools defined protection measures may not be applied and security risk may not be adequately managed.
Segregation of Duties	AEDA Tools must ensure proper segregation of conflicting duties to reduce the opportunity for unauthorized or unintentional modification or misuse of data or resources.	Inadequate segregation of duties can increase the impact of a malicious employee or compromised account.
Mobile Device Management	AEDA Tools must take special care when using mobile devices to ensure that sensitive information is not compromised, (e.g. using multi-factor authentication.)	Insufficient protection of mobile devices may increase the risk of mobile device compromise and unauthorized access to sensitive data.
Teleworking	AEDA Tools must implement a teleworking policy and supporting security measures to protect information accessed, processed, or stored offsite.	Insufficient protection during offsite work may increase the risk of unauthorized data access.
Pre-employment	AEDA Tools must conduct background checks all employment candidates. AEDA Tools' temp agencies must vet contractors. Employees and contractors must sign contracts that include responsibilities for information security.	Inadequate completion of worker verification and contracts may increase the risk of unauthorized data access from a malicious new hire.

Control Objective	Control Activity	Risk Statement
During Employment	AEDA Tools' management must ensure that personnel adhere to security requirements in their day-to-day operations. All employees, and where relevant, contractors must participate in security training and awareness activities.	Inadequate security training may result in inadequate or inconsistent application of security controls.
Disciplinary Process and Terminations	AEDA Tools must have human resources policies and procedures that disciplines employees that ignore or bypass information security controls.	Inadequate disciplinary processes may increase the risk of inadequate or inconsistent application of security controls from a noncomplying worker.
Inventory and Ownership of Assets	AEDA Tools is responsible for maintaining an inventory of assets. All assets must have an assigned business owner.	Informal and decentralized asset inventories can result in incorrect or missing asset information. This can lead to redundancies, extra costs and limited visibility for leadership into all Customer assets.
Acceptable Use and Return of Assets	AEDA Tools should have rules for acceptable use of its assets and processes for returns of asset upon termination of employment. Acceptable use processes must include USB blocking and DLP tools.	Improper management, use and protection of AEDA Tools assets may lead to data compromise
Classification, Labeling and Handling of Assets	AEDA Tools must classify information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure and modification. Classification schemas must include labeling and handling guidelines including data storage, transmission, and destruction requirements.	Inadequate asset handling may result in some assets receiving an inappropriate level of protection.
Management, Transfer and Disposal of Physical Media	AEDA Tools must have formal procedures in place for managing removable media and include security requirements. Any transportation of removable media must include processes to protect media in transit. AEDA Tools must dispose of removable media requires with destruction practices that render media unrecoverable.	Inadequate media handling may result in the unauthorized disclosure, modification, removal, or destruction of information.
Access Control Policies and Supporting Processes	AEDA Tools must establish and document an access control policy and key supporting processes.	Inadequate processes for managing user access may lead to unauthorized user access, loss, or compromise.

Control Objective	Control Activity	Risk Statement
User Lifecycle Management	AEDA Tools must maintain a formal, trackable, and auditable processes for managing user lifecycle that covers provisioning/deprovisioning of access. AEDA Tools must conduct periodic access reviews.	Inadequate processes for managing user lifecycles may lead to unauthorized user access, loss or compromise.
Authorization and Access Restrictions	In order to enforce need to know or need to use principles, AEDA Tools must restrict and control access via groups, roles, or permissions to information, application, and networks. AEDA Tools must limit administrator access to authorized individuals. AEDA Tools must strictly control access to networks and network services, utility programs, and application source code.	Improper access restrictions could lead to excessive access resulting in unauthorized access to resources and data compromise.
Password Handling	AEDA Tools must manage passwords through formal procedures. AEDA Tools must appropriately manage shared and service accounts. AEDA Tools must have interactive password management systems and must ensure quality passwords. AEDA Tools Personnel must be aware of their responsibilities regarding their password management.	Inadequately protected passwords increase the risk of account compromise.
User Access Configuration	AEDA Tools must ensure that user identities and passwords are sufficiently protected and follow creation and change requirements. AEDA Tools must configure system authentication to protect against attempted unauthorized access, credential capture, and detection of authentication system weaknesses.	Inadequate protection of authentication can increase the risk of account compromise.
Cryptographic Techniques	AEDA Tools must implement proper and effective cryptography techniques to protect the confidentiality, authenticity, and integrity of information. AEDA Tools must implement key management secure processes for generating, storing, archiving, retrieving, distributing, retiring, and destroying cryptographic keys.	Inadequate cryptographic controls may increase the risk of unauthorized disclosure of confidential data.

Control Objective	Control Activity	Risk Statement
Physical Security for Facilities and Sensitive Areas	AEDA Tools must define security perimeter controls and physical security requirements in accordance with the overall risk of the facility to provide sufficient protection. AEDA Tools must apply additional security controls and procedural requirements to sensitive areas such as data centers or clean rooms. AEDA Tools must design and apply protection against external and environmental threats.	Sensitive or critical information and information processing facilities may be insufficiently protected.
Physical Entry and Access Controls	AEDA Tools should protect secure areas by entry controls to ensure that only authorized personnel are allowed access. AEDA Tools should control access points such as delivery, loading areas, and other points where unauthorized persons could enter the premises.	Inadequate control of entry and access points to secure areas can increase the risk of unauthorized physical access, damage, and interference to information and information processing.
Cabling and Supporting Utilities	AEDA Tools must protect equipment from power failures and other disruptions caused by failures in supporting utilities. AEDA Tools should protect power and telecommunications cabling carrying data or supporting information services from interception, interference, or damage.	Inadequate protection of power and telecommunications infrastructure can increase the risk of system outages and unauthorized information disclosure.
Computing Equipment Management	AEDA Tools should site and protect equipment to reduce the risks from environmental threats, hazards, and opportunities for unauthorized access. AEDA Tools should properly maintain equipment to ensure its continued availability and integrity. AEDA Tools should apply security to off-site assets considering the different risks of working outside the organization's premises. AEDA Tools should not take off-site equipment, information, or software without prior authorization. AEDA Tools should verify all items of equipment containing storage to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Inappropriately maintained equipment may result in a loss of continued availability and integrity.

Control Objective	Control Activity	Risk Statement
Clean Desks and Clear Screens	AEDA Tools users should ensure that unattended equipment has protection. AEDA Tools should adopt a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities.	Employees may leave out confidential or restricted data in the view of individuals without the need to know. Employees without proper access rights can potentially access unlocked and unattended computers. Individuals without the need to know could view and exploit sensitive data. Maintenance staff could be exploited to steel sensitive information.
Documented Operating Procedures	AEDA Tools should document operating procedures and made available to all users who need them.	Inadequate procedural documentation can result in user errors, negative system impact, and data compromise.
Change Management	AEDA Tools should control changes to the organization, business processes, information processing facilities, and systems that affect information security. AEDA Tools should separate development, testing, and operational environments to reduce the risks of unauthorized access or changes to the operational environment. AEDA Tools should have carefully planned audit requirements and activities involving verification of operational systems.	Inadequate control of system change increases the risk of defects to production systems, which can degrade the security and protection of systems. Inadequate detection of changes can increase the potential damage caused by a malicious employee or compromised account with privileged access.
Capacity Management	AEDA Tools should monitor, tune, and make projections of future capacity of resource requirements to ensure the system performance.	Inadequate capacity management may increase the risk of inadequate system or capability delivery.
Information Backups	AEDA Tools should take and test backup copies of information, software, and system images in accordance with an agreed backup policy.	Inadequate or nonfunctional backups may increase the risk of data loss in the case of compromise, system malfunction, or environmental event.
Vulnerability Management	AEDA Tools should obtain information about technical vulnerabilities of information systems being used in a timely fashion, the organization's exposure to such vulnerabilities should be evaluated and measures taken to address the associated risk.	Lack of vulnerability management can increase the risk of asset compromise

Control Objective	Control Activity	Risk Statement
Logging and Monitoring	AEDA Tools must log, retain, and regularly review event logging, user activities, administrator/operator activities, exceptions, faults, and information security events. AEDA Tools must protect log data and clocks of all systems must be synchronized to a single reference.	Lack of logging and monitoring mechanisms may prevent discovery of unauthorized activity and lead to compromise.
Software Installation Management	AEDA Tools must have processes in place to control installation of software. AEDA Tools may not allow general users to install software on their own.	Users with admin access can circumvent change management due diligence and security measures, introducing unknown risk. Bypassing standard security measures for software selection creates unknown exposure to compromise. A malicious actor could exploit unknown vulnerabilities to access Customer's data.
Malware Management	AEDA Tools should implement detection, prevention, and recovery controls to protect against malware.	Lack of malware protection can increase the risk of asset compromise
Network Control	AEDA Tools must protect network management and services to ensure the availability, integrity, and confidentiality of information flowing through them.	Lack of protection measures around networks may lead to weak network infrastructure, unauthorized activity and compromise.
Network Design	AEDA Tools must design networks to segregate users, services, and information systems and restrict unauthorized traffic.	Inadequate network segmentation increases the risk of system compromise and unauthorized access.
Electronic Transfers of Information	AEDA Tools must adequately protect the transfer of information internally and with external partners with technical, procedural, and contractual controls applied as appropriate.	Inadequate protection and control of information transfers increases the risk of unauthorized data disclosure.
Information Security Requirements in SDLC	AEDA Tools must include the information-security-related requirements in the due diligence when implementing new information systems or enhancements to existing information systems.	New tools and efforts may not consider all security requirements, which could result in a vulnerable product or process.

Control Objective	Control Activity	Risk Statement
Protection for Publicly Available Applications and Application Transactions	AEDA Tools must protect applications available over public network from fraudulent activity, contract dispute, unauthorized information disclosure, and modifications. AEDA Tools must protect transactions to prevent incomplete transmission, mis-routing, unauthorized activities (messaging, alterations, disclosure, message duplication, or replay).	Insufficient protection of public applications may increase the risk of compromise.
SDLC Governance	AEDA Tools development teams must assure of the integrity and quality of delivered systems and software products. They must document and govern the way they write and manage code, including secure development practices, code build and promotion, defect handling, and assess third-party components for use.	Inadequate code control and quality can increase the risk of compromised or vulnerable software.
Software Supply Chain Management	AEDA Tools must cover software development and system maintenance processes on all third-party software components. AEDA Tools should use standard maintained secure baselines to consistently configure software when possible, and modification of software components should be avoided. AEDA Tools should manage patches and defect fixes to software components as part of the security of the overall system or software product.	Inadequately managed software components may increase the risk of vulnerabilities in systems and software.
Development Environments and Protection of Test Data	AEDA Tools must establish and protect development environments based on the type of development work being performed. AEDA Tools must carefully select and manage test data.	Inadequate management and protection of test environments and data may increase the risk of unauthorized data access and defects in production systems.
System and Application Testing	AEDA Tools must test systems and applications when significant changes are made. AEDA Tools must include testing of security functions in the development cycle. AEDA Tools must conduct acceptance testing before any systems are released as live.	Inadequate change testing may increase the risk of security defects in production systems.

Control Objective	Control Activity	Risk Statement
Information Security Requirements for Vendors and Sub vendors	AEDA Tools documents and mutually agrees on information security requirements for mitigating risks associated with vendors. These requirements are especially critical for any vendors that accesses, processes, stores, transmits, or communicates Customer data or provides IT infrastructure components for Customer. The AEDA Tools must propagate or trickle down requirements to all vendors and sub vendors providing services to Customer.	Inadequate management of vendor security practices may increase the risk of compromise or unauthorized access of Customer data while in use by a vendor.
Ongoing Management of Vendors and Vendor Relationships	AEDA Tools must regularly monitor and assess vendors to ensure that they are still meeting established security requirements. AEDA Tools must review and reassess any changes to vendor relationships for new risk considering type of change and criticality of information and systems involved.	Inadequate assessment of vendor security may increase the risk of compromise or unauthorized access of Customer data while in use by a vendor.
Incident Management	AEDA Tools must identify and define roles and responsibilities, including identification of individuals required to maintain contact with authorities. AEDA Tools must assess and determine if information security events classify as incidents. AEDA Tools must address incidents timely and appropriately based on documented procedures. AEDA Tools' incident management processes must include procedures for collection of evidence.	Inadequate preparation for security incidents can increase the impact and cost of security incidents.
Incident Reporting	AEDA Tools must report information security events/incidents as well as any weaknesses in systems or services reported in a timely manner via appropriate channels.	AEDA Tools leadership is unaware of the risk associated with each event. The business is unable to use the full resources and tools of AEDA Tools' incident response team. As a result, the impact of security incidents may be greater than they would be if AEDA Tools was fully involved.
Incident Post Mortem Analysis	AEDA Tools should use knowledge gained from analyzing and resolving information security incidents to reduce the likelihood or impact of future incidents.	Inadequate analysis of incident may increase the risk of repeat incidents.

Control Objective	Control Activity	Risk Statement
Business Continuity Planning	AEDA Tools must incorporate Business Continuity Plans and initiatives in information security and technical security components. AEDA Tools must place processes and procedures to ensure that security controls are maintained throughout an adverse event.	Lack of business continuity planning can lead to loss or compromise because of a disaster.
Business Continuity Testing	AEDA Tools must test Business Continuity Plans periodically to ensure that they are still valid and effective during adverse situations.	Lack of recovery testing will not provide validation that existing recovery controls are enough to address recovery needs.
Availability and Redundancy of Systems and Facilities	AEDA Tools must place sufficient redundancy to meet availability requirements as defined in recovery time and point objectives.	Inadequate or nonfunctional redundancy may increase the risk of data loss in the case of compromise, system malfunction, or environmental event.
"Managing Statutory, Regulatory and Contractual Requirements "	AEDA Tools must implement legislative statutory, regulatory, and contractual requirements as well as processes for meeting those requirements. AEDA Tools must include processes for approaches to managing intellectual property rights, protection of organizational records, and privacy/protection of personally identifiable information.	Inadequate legal compliance may increase the risk of legal or regulatory action, termination of business partnerships, or enforced renegotiation of contracts with less beneficial terms.
Information Security Reviews	AEDA Tools must perform independent reviews of information security and technical security requirements to ensure compliance with security policies and standards.	Inadequate assurance can increase the risk of incorrectly, inadequately, or inconsistently applied security controls.

EXHIBIT D

GDPR Addendum

This GDPR Addendum (the "***GDPR Addendum***") applies to the Master Services Agreement (the "***Agreement***") dated _____ and forms a part of the Agreement and all other agreements between Customer Corporation ("***Customer***") and _____ and/or its affiliates ("***AEDA Tools***"). This GDPR Addendum is effective as of _____ or **the date of full execution, whichever is earlier**. Customer is entering into this GDPR Addendum on behalf of itself and for the benefit of its customers. The AEDA Tools is providing services to and for the benefit of Customer. THIS GDPR ADDENDUM GOVERNS THE DATA PROCESSING OPERATIONS BETWEEN CUSTOMER AND SERVICE PROVIDER.

With respect to provisions regarding processing of Personal Data, in the event of a conflict between the Agreement and this GDPR Addendum, the provisions of this GDPR Addendum shall control.

"Data Protection Legislation"	Shall mean all applicable laws relating to data protection and privacy including (without limitation) the EU Data Protection Directive (95/46/EC) as implemented in each jurisdiction, the EU General Data Protection Regulation (2016/679), the EU Privacy and Electronic Communications Directive 2002/58/EC as implemented in each jurisdiction, and any amending or replacement legislation from time to time.
"Personal Data"	Shall mean all personal data (as defined in the Data Protection Legislation) controlled by Customer which is processed by the AEDA Tools in connection with the Services;

1. DATA PROTECTION

In this clause, the terms "personal data", "process", "data controller", "data processor", "data subject" and "supervisory authority" shall have the meanings set out in the Data Protection Legislation.

1.1. The AEDA Tools is appointed by Customer to process Personal Data on behalf of Customer as is necessary to provide the Services and in accordance with such other written instructions as Customer may issue from time to time.

1.2. Each party shall comply with its obligations under the Data Protection Legislation in respect of any Personal Data it processes under or in relation to this Agreement. Without prejudice to the foregoing, the AEDA Tools shall not process Personal Data in a manner that will or is likely to result in Customer breaching its obligations under the Data Protection Legislation.

1.3. The subject-matter, duration, nature and purpose of the processing, together with the categories of data subjects and type of Personal Data to be processed by the AEDA Tools under this Agreement are set out in Schedule 1.

1.4. The AEDA Tools warrants and undertakes in respect of all Personal Data that at all times it shall:

(a) only process Personal Data in accordance with the documented instructions given from time to time by Customer, including with regard to transfers, unless required to do otherwise by applicable law. In which event, the AEDA Tools shall inform Customer of the legal requirement before processing Personal Data other than in accordance with Customer's instructions, unless that same law prohibits the AEDA Tools from doing so on important grounds of public interest;

(b) notify Customer prior to taking any further action if it considers an instruction is likely to result in processing that is in breach of Data Protection Legislation;

(c) implement technical and organisational measures to protect any Personal Data processed by it against unauthorised and unlawful processing and against accidental loss, destruction, disclosure, damage or alteration. This shall include, as a minimum, the security requirements set out in Schedule 2;

(d) not publish, disclose or divulge (and ensure that its personnel do not publish, disclose or divulge) any Personal Data to a third party unless Customer has given its prior written consent;

(e) ensure that only such of its personnel who may be required by the AEDA Tools to assist it in meeting its obligations under this Agreement will have access to Personal Data and that such personnel are bound by obligations of confidentiality, and take all reasonable steps in accordance with industry practice to ensure the reliability of such personnel;

(f) inform Customer promptly, and in any event within two (2) business days, of any enquiry or complaint received from a data subject or supervisory authority relating to Personal Data;

(g) at no additional cost, provide full cooperation and assistance to Customer as Customer may require to allow Customer to comply with its obligations as a Data Controller, including in relation to data security; data breach notification; data protection impact assessments; prior consultation with supervisory authorities; the fulfilment of data subject's rights; and any enquiry, notice or investigation by a supervisory authority; and

(h) at the request and option of Customer (whether during or following termination of this Agreement), promptly and as specified by Customer return or destroy all Personal Data in the possession or control of the AEDA Tools.

1.5. Notwithstanding any provisions of the Agreement, the AEDA Tools may not appoint any third party to process Personal Data ("***Subprocessor***") unless it does each of the following:

(a) providing reasonable prior notice to Customer of the identity and location of the Subprocessor and a description of the intended processing to be carried out by the Subprocessor to enable Customer to evaluate any potential risks to Personal Data; and

(b) imposing legally binding contract terms on the Subprocessor which are the same as those contained in this Agreement.

Otherwise, AEDA Tools may appoint and use Subprocessors in its discretion.

1.6. The AEDA Tools acknowledges and agrees that it shall remain liable to Customer for a breach of the terms of this Agreement by a Subprocessor and other subsequent third-party processors appointed by it.

2. SECURITY BREACHES

2.1. The AEDA Tools shall notify Customer in the most expedient time possible under the circumstances and in any event within 24 (twenty-four) hours of becoming aware of any actual or suspected accidental,

unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Personal Data ("***Security Breach***"). The AEDA Tools shall also provide Customer with a detailed description of the Security Breach, the type of data that was the subject of the Security Breach and (to the extent known to the AEDA Tools) the identity of each affected person(s), as soon as such information can be collected or otherwise becomes available, as well as all other information and co-operation which Customer may reasonably request relating to the Security Breach.

2.2. The AEDA Tools agrees to take action immediately, at its own expense, to investigate the Security Breach and to identify, prevent and mitigate the effects of any such Security Breach and, with Customer's prior agreement, to carry out any recovery or other action necessary to remedy the Security Breach.

2.3. The AEDA Tools may not issue, publish or make available to any third party any press release or other communication concerning a Security Breach without Customer's prior approval.

3. DATA TRANSFERS

3.1. Customer hereby consents to Personal Data being processed outside the EEA, subject to the AEDA Tools' continued compliance with clause 1.12 and clause 1.13 throughout the duration of this Agreement.

3.2. To the extent that any Personal Data is processed outside the EEA, the terms of the transfer shall be governed by the EU Standard Contractual Clauses for the transfer of personal data to processors attached as Schedule 3, which are hereby incorporated into this Agreement.

3.3. If, for whatever reason, the transfer of Personal Data ceases to be lawful, the AEDA Tools shall either:

(a) with Customer's consent, implement an alternative lawful transfer mechanism; or

(b) allow Customer to terminate the Agreement at no additional cost to Customer.

3.4. The AEDA Tools shall make available to Customer all information necessary to demonstrate its compliance with Data Protection Legislation and allow for and contribute to audits, including physical inspections, conducted by Customer or its representatives bound by obligations of confidentiality.

3.5. The AEDA Tools shall indemnify and keep Customer fully and effectively indemnified in respect of all losses, damages, costs, charges, expenses and liabilities (including regulatory penalties imposed on Customer) arising out of or in connection with a breach by the AEDA Tools of its obligations under Data Protection Legislation.

4. General

4.1. **En***tire Agreement*: This GDPR Addendum and the Agreement together constitute the entire agreement between the Parties with respect to the subject matter of this GDPR Addendum and supersede and extinguish any prior drafts, agreements, undertakings, understandings, promises or conditions, whether oral or written, express or implied between the Parties relating to such subject matter.

4.2. ***Counterparts***: This GDPR Addendum may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.

4.3. ***Waivers:*** Delay in exercising or non-exercise of any right under this GDPR Addendum is not a waiver of that or any other right. Partial exercise of any right under this GDPR Addendum shall not preclude any further or other exercise of that right or any other right under this GDPR Addendum. Waiver of a breach of any term of this GDPR Addendum shall not operate as a waiver of breach of any other term or any subsequent breach of that term.

4.4. ***Precedence***: In the event of a conflict between any of the terms of this GDPR Addendum, the Agreement and the Model Clauses (if applicable) the conflict shall be resolved according to the following descending order of priority: (i) the Model Clauses (if applicable), (ii) the clauses of this GDPR Addendum, then (iii) the Agreement.

4.5. ***Survival of obligations:*** Notwithstanding any provision of this GDPR Addendum to the contrary, the provisions of clause 1.14 and any other clauses which expressly or impliedly survive expiry or termination of this GDPR Addendum for any reason whatsoever shall continue in full force and effect after expiry or termination.

4.6. ***Governing law and jurisdiction:*** This GDPR Addendum and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of Ireland. Each party irrevocably agrees that the courts of Ireland shall have the exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this GDPR Addendum or its subject matter or formation (including non-contractual disputes or claims).

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

This GDPR Addendum is entered into and becomes a binding part of the Agreement with effect from the date first set out above.

CUSTOMER CORPORATION

Signature _____

Name _____

Title _____

Date Signed _____

SERVICE PROVIDER – PLEASE INSERT NAME

Signature _____

Name _____

Title _____

Date Signed _____

Schedule 1: Description of Personal Data Processing

The data processing activities carried out by the AEDA Tools may be described as follows:

1. **Subject Matter**

   [Provide a brief description of the subject matter of the processing, i.e. the subject matter of the Service Agreement as it involves personal data]

2. **Duration**

   [*Insert duration of the processing*]

3. **Nature and purpose**

   [*Describe the type of processing and its purpose(s)*]

4. **Data Categories**

   [Insert the types of personal data which are subject to the processing]

5. **Data Subjects**

   [Insert the categories of data subjects who are subject to the processing]

Schedule 2: Security Requirements

AEDA Tools will abide by Customer's security requirements as found at:

https://www.deluxe.com/sites/deluxe.signupserver.com/files/MSA-Exhibit-for-TPSP-Requirements-v2.pdf

Schedule 3: Standard Contractual Clauses for transfers from Controller to Processors

The following Schedule will be used when Personal Data leaves the EEA that is processed by AEDA Tools and enters countries that do not have adequate data protections in place.

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection.

Data Exporter:
Address:
Tel. _____ fax _____; e-mail: _____

Data Importer:
Address:
Tel. _____ fax _____; e-mail: _____

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the "***Clauses***") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1];

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of

individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-

processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely Ireland.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data

importer under the Clauses [3]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely Ireland.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

FURTHER PROVISIONS:

A. General Data Protection Regulation

A.1. Except as set out in Section B.1 below, upon the repeal and replacement of Directive 95/46/EC (the "**Directive**") by the General Data Protection Regulation (2016/679) (the "**Regulation**"), references throughout these Clauses to the Directive shall be read as references to the Regulation.

B. Execution Process

This Agreement may be executed in counterparts and it shall not be necessary that the signatures of all parties hereto be contained on any one counterpart hereof; each counterpart shall be deemed as original, but all of such counterparts together shall constitute one and the same instrument. This Agreement may be executed in duplicate, each of which is an original. A legal agreement shall be formed from the Effective Date between each data exporter (who has signed and returned a counterpart) on the one hand and each and every data importer (who has signed and returned a counterpart).

ON BEHALF OF THE DATA EXPORTER:

Signature: _____

Name: _____

Position: _____

Address: _____

ON BEHALF OF DATA IMPORTER SERVICE PROVIDER PLEASE INSERT NAME:

Signature: _____

Name: _____

Position: _____

Address: _____

Appendix 1 to the Standard Contractual Clauses

Data exporter:

The data exporter provides wholesale websites to large-scale telecommunications companies and others via white-label services and is also a retail provider of websites.

Data importer: AEDA Tools Please Insert Name

The data importer is (please specify briefly activities relevant to the transfer):

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

- retail customers' personal data
- wholesale partners' customer data

Categories of data

The personal data transferred concern the following categories of data (please specify):

- First Name, Last Name;
- Email Address;
- Domain Name;
- Username;
- Password

Special categories of data (if appropriate)

No special categories of data are collected.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

- Network Operations
- Software Development
- Technical Support
- Web Design

Retention Period

AEDA Tools and its processors will retain the data for the duration of the Services.

Approved Sub-Processors

PURPOSE OF THE PROCESSING	CATEGORIES AND ESTIMATED VOLUME OF PERSONAL DATA	DATA SUBJECTS	LOCATION OF THE PROCESSING	APPROVED SUB-PROCESSOR	RETENTION PERIOD FOR THE PERSONAL DATA

	PROCESSED				

DATA EXPORTER

Print Name: _____

Authorised Signature: _____

DATA IMPORTER AEDA Tools Please Insert Name

Print Name: _____

Authorized Signature: _____

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

DATA EXPORTER

Print Name: _____

Authorised Signature: _____

DATA IMPORTER AEDA Tools Please Insert Name

Print Name: _____

Authorised Signature: _____