FINALSITE DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") constitutes an integral part of all agreements ("**Agreement**") by and between **ACTIVE INTERNET TECHNOLOGIES, LLC dba Finalsite**, a Connecticut limited Liability Company with offices at 655 Winding Brook Drive, Glastonbury, Connecticut, 06033 ("**Finalsite**") and the contracting party identified on the signature page of the relevant Order as the Customer ("**Customer**") (jointly "**the Parties**", and each a "**Party**"), including the Master Terms and Conditions ("**Master Terms**"), each fully executed Order and Statement of Work, or under any services agreement or similar agreement (collectively, "**Agreement**"). This DPA reflects the Parties' agreement with regard to the Processing of Customer Data in accordance with the requirements of Data Protection Laws and the Federal Acquisition Regulation.

This DPA is effective on the date that it has been duly executed by both Parties ("**Effective Date**"), and amends, supersedes and replaces any prior agreement relating to data processing and/or data protection the Parties entered into. Capitalized terms not otherwise defined in this DPA shall have the meanings ascribed to them in the Master Terms.

If the Customer is an ordering activity under Governmentwide Acquisition Contracts ("GSA Schedule Contracts"), it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Addendum, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. DEFINITIONS

- In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1 "**Applicable Data Protection Laws**" means all laws or regulations applicable to the Customer Data.

1.2 **"Controller"** means the entity that determines the purposes and means of the Processing the Customer Data.

1.3 **"Processor"** means the entity that Processes Customer Data.

1.4 **"Data Subject"** means the identified or identifiable person to whom the Customer Data relates.

1.5 **"Data Subject Rights"** means all rights granted to Data Subjects by Applicable Data Protection Laws.

1.6 **"Customer"** means the entity that executed the Agreement which determines the purposes and means of the Processing of Customer Data.

1.7 "**Customer Data**" means any Personal Data Processed by Processor on behalf of Customer pursuant to or in connection with the Agreement.

1.8 "**Personal Data**" means any information relating to an identified or identifiable natural person that relates to, describes, is capable of being associated with, or could be linked, directly or indirectly, with a particular natural person.

1.9 **"Processing"** means any operation or set of operations which is performed upon Customer Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.10 **"Security Breach"** means any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure or destruction of Customer Data stored on Finalsite's equipment or in Finalsite's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data stored by a Finalsite Subprocessor.

1.11 "**Security Practices Document**" means the Information Security Practices Document (or the applicable part dependent on what Services Customer purchases from Finalsite), as updated from time to time, and made available to Customer on request.

1.12 "**Services**" means the provision of maintenance and support services, consultancy or professional services and the provision of software as a service or any other services provided under the Agreement where Finalsite Processes Customer Data.

1.13 "**Subprocessor**"means any data processor (excluding an employee of Finalsite or any of its sub-contractors) appointed by or on behalf of Finalsite to Process Personal Data on behalf of Customer in connection with the Agreement.

1.14 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. AUTHORITY

2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Customer Data, Customer is the Controller while Finalsite is the Processor.

2.2 **Controlling Agreement.** This DPA supplements the Agreement and in the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA prevail.

3. PROCESSING OF CUSTOMER DATA

3.1 Finalsite shall comply with all Applicable Data Protection Laws in the Processing of Customer Data. Finalsite shall not Process Customer Data other than on the Customer's documented instructions unless Processing is required by Applicable Data Protection Laws to which the Finalsite is subject, in which case Finalsite shall, to the extent permitted by Applicable Data Protection Laws, inform Customer of that legal requirement before the relevant Processing of that Customer Data.

3.2 Customer warrants that it shall, in its use of the Services, Process Customer Data in accordance with Applicable Data Protection Laws, including any requirement to provide notice to Data Subjects of its use of Finalsite as Processor. Customer further warrants that its instructions for the Processing of Customer Data pursuant to this DPA comply with the Applicable Data Protection Laws. Customer instructs Finalsite to Process Customer Data as reasonably necessary for the provision of the Services and consistent with the Agreement; and warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out herein.

3.3 **Details of Processing Activities**. The subject matter of Processing of Customer Data by Finalsite is the performance of the Service pursuant to the Agreement.

4. FINALSITE'S OBLIGATIONS

4.1 **Confidentiality**. Finalsite shall ensure that its personnel engaged in the Processing of Customer Data are informed of the confidential nature of the Customer Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Finalsite shall ensure that such confidentiality obligations survive the termination of the personnel engagement. Finalsite shall ensure that access to Customer Data is limited to those personnel performing Services in accordance with the Agreement on a need-to-know basis.

4.2 **Data Subject Requests.** Finalsite shall, to the extent legally permitted, promptly notify Customer if Finalsite receives a request from a Data Subject to exercise a Data Subject Request. Finalsite will assist the Customer by implementing reasonable technical and organisational measures, insofar as this is possible, to fulfil Customer's obligation to respond to requests for exercising Data Subject rights under Applicable Data Protection Laws. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Finalsite shall upon Customer's request provide commercially reasonable assistance to Customer in responding to such Data Subject Request, to the extent Finalsite is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Finalsite's provision of such assistance.

4.3 **Disclosure to Third Parties.** Finalsite will not disclose Customer Data to third parties except as permitted by this DPA or the Agreement, unless Finalsite is legally required to disclose Customer Data, in which case Finalsite shall, to the extent legally permitted, notify Customer in writing and liaise with Customer before complying with such disclosure request.

4.4 **Retention**. Finalsite will retain Customer Data only for as long as Customer deems it necessary for the purposes of Processing, or as required under the applicable law. At the termination of this DPA, or upon Customer's written request, Finalsite will either destroy or return Customer Data to Customer, unless legal obligations require storage of Customer Data.

4.5 **Security.** Finalsite shall maintain appropriate administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, such measures are set out in Appendix 1 of this DPA. Finalsite monitors compliance with these safeguards. In assessing the appropriate level of security, Finalsite shall take account, in particular, of the risks that are presented by Processing.

4.6 **Government Contracting.** As prescribed by the General Services Administration contracting requirements and the Federal Acquisition Regulations Privacy Act Provisions, the following clauses shall apply to this Agreement:

4.6.1 **Privacy Act Notification.** Finalsite will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

4.6.2 **Privacy Act.**

i. Finalsite agrees to:

(a) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(b) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the design, development, or operation of a system of records on individuals that is subject to the Act; and

(c) Include this clause, including this paragraph (c), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(d) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, Finalsite is considered to be an employee of the agency.

(e) Definitions:

(i) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(ii) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(iii) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

5. THIRD PARTY CERTIFICATION AND AUDITS

5.1 **Certifications**. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Finalsite shall make available to Customer a copy of Finalsite's then most recent third-party audits or certifications, as applicable.

5.2 **Audits**. Customer may contact Finalsite to request an audit of Finalsite's procedures relevant to the protection of Customer Data, but only to the extent required under Applicable Data Protection Laws. Such

audit will be conducted by an independent third party reasonably acceptable to Finalsite. Before the commencement of any such on-site audit, Customer and Finalsite shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. Such audits will not occur more than annually. The results of the inspection and all information reviewed during such inspection will be deemed Finalsite's confidential information and shall be protected by the auditor in accordance with the confidentiality obligations set forth in the Agreement. Notwithstanding any other terms, the auditor may only disclose to Customer specific violations of the DPA, if any, and the basis for such findings, and shall not disclose any of the records or information reviewed during the inspection to Customer.

6. SUB-PROCESSING

6.1 **General Consent.** Customer acknowledges and agrees that Finalsite may engage third-party Subprocessors in connection with the provision of the Services subject to the conditions noted in this section. As a condition of engaging Subprocessors, Finalsite will enter into a written agreement with each Subprocessor containing data protection obligations, including security measures, not less protective than those in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the services provided by such Subprocessor.

6.2 **Consent to Subprocessor Engagement.** Customer acknowledges and agrees that Finalsite may engage its current Subprocessors listed in Finalsite's customer portal on its website. Without prejudice to Section 6.3, Customer generally authorizes the engagement as Subprocessor of any other third parties.

6.3 **Notification of New Subprocessors and Customer Objection**. During the term of the Agreement, Finalsite will update its current Subprocessor list in the customer portal on its website periodically to reflect any changes. Finalsite will notify Customer if it adds or removes Subprocessors if Customer has notified Finalsite in writing that it wishes to receive such notifications.

6.4 **Liability**. Finalsite shall be liable for the acts and omissions of its Subprocessors to the same extent Finalsite would be liable if performing the services of each Subprocessor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

7. SECURITY BREACH

7.1 If Finalsite becomes aware of a Security Breach, Finalsite will promptly: (a) notify Customer of the Security Breach; (b) investigate the Security Breach and provide Customer with information about the Security Breach; and (c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach. Finalsite's obligation to report or respond to a Security Breach under this Section is not and will not be construed as an acknowledgement by Finalsite of any fault or liability with respect to the Security Breach.

7.2 Notification(s) of Security Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means Finalsite selects, including via email. It is Customers's sole responsibility to ensure it maintains accurate contact information on Finalsite's support systems at all times.

8. LIMITATION OF LIABILITY

Each Party's liability arising out of or related to this DPA whether in contract, tort or under any other theory of liability, is subject to the 'Liability Limit' section of the Master Terms, and any reference in such section to the liability of a Party means the aggregate liability of that Party under the Agreement and all DPAs together.

- For the avoidance of doubt, Finalsite's total liability for all claims from Customer arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement.

9. OBLIGATIONS POST-TERMINATION

- Termination or expiration of this DPA shall not discharge the Parties from their obligations meant to survive the termination or expiration of this DPA.

10. SEVERABILITY

- Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The Parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this DPA.

IN WITNESS WHEREOF, the Parties hereto, as evidenced by the signatures below, have executed this DPA as of the Effective Date.

ACTIVE INTERNET TECHNOLOGIES, LLC	**[GOVERNMENT ENTITY NAME]**
d/b/a Finalsite	
By:_____	By: _____
Name:_____	Name: _____
Title: _____	Title: _____
Date Signed: _____	Date Signed: _____

■ APPENDIX 1 - TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

This Appendix sets forth a description of the technical and organisational measures implemented by Finalsite which are designed to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Finalsite will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data uploaded to the Services, as applicable to the specific Finalsite Services purchased by data exporter. Finalsite will not materially decrease the overall security of the Finalsite Services during a subscription term.

Finalsite implements the following measures to safeguard Customer Data:

- Encryption. Finalsite encrypts Customer Data while in transit and at rest using industry-standard encryption technologies.
- Confidentiality, integrity, availability and resilience of processing systems. Finalsite utilises Google Cloud or Amazon Web Services to host its applications across multiple availability zones; Finalsite utilises automatic fail-over systems for certain applications and internal systems; Finalsite conducts regular hourly and daily backups of Customer Data, as well as other industry-standard safeguards for ensuring resilience of processing systems. Finalsite performs regular vulnerability scanning of its software applications and has continuous managed threat detection in place.
- Data Restoration. Finalsite utilises automatic fail-over systems for certain applications and internal systems; Finalsite conducts regular backups of Customer Data designed to facilitate timely recovery in the event of a service interruption. In addition, Finalsite's third-party cloud hosting providers deploy replicated systems for physical redundancies spanning multiple geographic zones.
- Testing, assessing and evaluating the effectiveness of technical and organisational measures. Finalsite performs periodic testing of its technical and organisational measures, and Finalsite's third party hosting providers perform regular testing of physical security measures. Finalsite continuously monitors its systems for malware utilizing industry-standard managed threat detection. Finalsite conducts annual independent penetration testing of its systems and applications to identify and resolve foreseeable attack vectors and potential cyber threats.
- Access Controls. Finalsite requires Customers to utilise unique usernames and passwords for access to its applications; Finalsite enables termination of access credentials by deleting user accounts and access when users leave the Customer's organization. Internally, Finalsite limits access to Customer Data to those employees and subprocessors with a need to know.
- Physical security. Finalsite utilises Google Cloud and Amazon Web Services to host its software applications, which deploy industry-standard physical security measures concerning the hosting environments at which Customer Data is physically stored. Finalsite employee computers accessing Customer Data are encrypted utilizing industry- standard means.
- Events logging. Finalsite enables systems logging in connection with its threat monitoring and detection activities. Finalsite utilises request logging of all incoming user traffic in its applications, as well as Customer admin and employee access activity.
- IT security governance and management. Finalsite maintains written policies and procedures for IT security governance and management.
- Data minimisation. Finalsite does not enable collection of sensitive personal data in its applications except where necessary to provide the specific services to Customers.

- Data quality. Finalsite's applications regularly test certain data fields for validity and reject invalid data before processing and storge.
- Training. Finalsite conducts privacy and security awareness training for all new hires and periodic privacy and security awareness training for employees and contractors who have access to Customer Data.
- Data erasure and destruction. Customer Data is deleted within Finalsite's applications upon service termination or Customer request; backups are deleted automatically on a regular basis in accordance with Finalsite's formal data retention policy.
- Vendor Management. Finalsite enters into formal agreement s with its subprocessors containing industry-standard data protection provisions consistent with those measures deployed by Finalsite.

APPENDIX 2 - LIST OF SUBPROCESSORS

Customer has authorised the use of the following sub-processors:

Information about Subprocessors, including their functions, contact details, and locations, is available at: https://www.finalsite.com/subprocessors (as may be updated by Finalsite from time to time in accordance with this DPA).