DATA PROCESSING ADDENDUM

United States

This Data Processing Addendum (including the annexes attached hereto, this "DPA") is hereby incorporated into the Agreement (as defined below) as of the Addendum Effective Date (as defined below) between the undersigned Party ("Customer") and Nuclei, Inc. ("Nuclei"). Customer and Nuclei may be referred to herein individually as a "Party" and collectively as the "Parties".

1. Definitions and Interpretation.

For purposes of this DPA, the terms below have the meanings set forth below. Capitalized terms that are used but not defined in this DPA have the meanings given in the Agreement.

1.1. Addendum Effective Date means the effective date of the Agreement as of the date signed by both Parties.

1.2. Agreement means the Nuclei Subscription Agreement or Business Partner Agreement, as applicable, entered into by and between the Parties.

1.3. Affiliate means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

1.4. Applicable Data Protection Laws means the privacy, data protection and data security laws and regulations of any jurisdiction within the United States applicable to Nuclei's Processing of Personal Data under this DPA, including, as and to the extent applicable, the State Privacy Laws.

1.5. CCPA means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (the "CPRA"), and any binding regulations promulgated thereunder.

1.6. CDPA means the Virginia Consumer Data Protection Act.

1.7. CPA means the Colorado Privacy Act.

1.8. Customer Data means the entirety of information provided or made available by Customer to Nuclei for Processing on Customer's behalf to perform the Services. It may or may not contain Personal Data.

1.9. Data Subject means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.10. Data Subject Request means the exercise by a Data Subject of their rights under, and in accordance with, Applicable Data Protection Laws in respect of Customer Data.

1.11. Information Security Incident means a breach of Nuclei's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Nuclei's possession, custody or control. Information Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

1.12. PDPOM means the Connecticut Act Concerning Personal Data Privacy and Online Monitoring.

1.13. Personal Data means Customer Data that constitutes 'personal data', 'personal information', or 'personally identifiable information' as defined in Applicable Data Protection Laws or information of a similar character regulated thereby, attributable to a Data Subject.

1.14. Processing means any operation or set of operations which is performed by (or on behalf of Nuclei) on behalf of Customer under this DPA, on Personal Data or on sets of Personal Data, whether or not by automated 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.

1.15. Security Measures has the meaning given in Section 4(a) (Nuclei's Security Measures).

1.16. Services means any services provided by Nuclei to Customer pursuant to the Agreement.

1.17. State Privacy Laws means, collectively, the CCPA, CDPA, CPD, CPRA, PDPOM and UCPA.

1.18. Subprocessors means third parties that Nuclei engages to Process Personal Data in relation to the Services.

1.19. Third-Party Subprocessors has the meaning given in Section 7 (Subprocessors).

1.20. UCPA means the Utah Consumer Privacy Act.

2. Duration and Scope of DPA.

This DPA will remain in effect so long as Nuclei Processes Personal Data, notwithstanding the expiration or termination of the Agreement.

Processing of Personal Data subject to the State Privacy Laws with respect to which Customer is a Business, Controller, Processor, or Service Provider (as such terms are defined in State Privacy Laws) shall be subject to Annex 1 (State Privacy Laws Annex) to this DPA.

3. Customer Instructions.

Nuclei will Process Personal Data only in accordance with Customer's instructions to Nuclei. This DPA is a complete expression of such instructions, and Customer's additional instructions will be binding on Nuclei only pursuant to an amendment to this DPA signed by both Parties. By entering into this DPA, Customer instructs Nuclei to Process Personal Data to provide the Services and to perform its other obligations and exercise its rights under the Agreement.

4. Security and Incidents.

4.1. Nuclei Security Measures. Nuclei will implement and maintain technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data (the "Security Measures") as described in Annex 2 (Security Measures). Nuclei may update the Security Measures from time to time, so long as the updated measures do not decrease the overall protection of Personal Data.

4.2. Security Compliance by Nuclei Staff. Nuclei shall require that its personnel who are authorized to access Personal Data are subject to appropriate confidentiality obligations.

4.3. Information Security Incidents. Nuclei will notify Customer without undue delay of any Information Security Incident of which Customer becomes aware. Such notifications will describe available details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Nuclei recommends Customer take to address the Information Security Incident. Nuclei's notification of or response to an Information Security Incident will not be construed as Nuclei's acknowledgement of any fault or liability with respect to the Information Security Incident.

5. Data Subject Rights.

5.1. Nuclei shall, upon Customer's reasonable written request, provide Customer with such assistance as may be reasonably necessary and technically possible in the circumstances to assist Customer in fulfilling its obligation to respond to Data Subject Requests.

5.2. Notwithstanding the foregoing, Customer acknowledges and agrees that the Services may offer functionality for Customer to export Customer Data records without assistance from Nuclei, and Customer shall attempt to use any such self-serve functionality before requesting Nuclei's assistance with any Data Subject Request.

5.3. Upon receipt of any Data Subject Request that relates to Customer Data that Nuclei Processes for Customer, Nuclei shall promptly notify Customer and not respond to such Data Subject Request except on the written instructions of Customer.

5.4. Customer is solely responsible for responding to Data Subject Requests. Due to the nature of the Processing of Personal Data in certain industries, the implementation of Data Subject Requests may be limited by applicable laws and regulations.

5.5. Nuclei's notification of, or response to, a Data Subject Request pursuant to this Paragraph is not an acknowledgement by Nuclei of any fault or liability with respect to the relevant Data Subject Request.

6. Customer Responsibilities.

6.1. Customer shall ensure (and is solely responsible for ensuring) that it has given such notices to and obtained such consents and permissions from third parties (including, without limitation, Data Subjects), and has reserved all rights, in each case, as may be required under applicable law or otherwise for Nuclei to Process Personal Data as contemplated by the Agreement.

6.2. Customer represents and warrants to Nuclei that Customer Data does not and will not contain any social security numbers or other government-issued identification numbers, protected health information subject to the Health Insurance Portability and Accountability Act ("HIPAA") or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health insurance information; biometric information; passwords for online accounts; credentials to any financial accounts; tax return data; any payment card information subject to the Payment Card Industry Data Security Standard; personal data of children under 13 years of age; or any other information that falls within any special categories of protected data (as defined in Applicable Data Protection Laws).

6.3. Customer's Security Responsibilities. Customer agrees that, without limitation of Nuclei's obligations under Section 4 (Security), Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; (c) securing Customer's systems and devices that Nuclei uses to provide the Services; and (d) backing up Personal Data.

6.4. Customer's Security Assessment. Customer agrees that the Services, the Security Measures and Nuclei's commitments under this DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Personal Data.

7. Subprocessors.

7.1. Consent to Subprocessor Engagement. Customer specifically authorizes the engagement of Nuclei's Affiliates as Subprocessors and generally authorizes the engagement of any other third parties as Subprocessors ("Third-Party Subprocessors").

7.2. Information about Subprocessors. Nuclei shall inform Customer of any intended changes concerning the addition or replacement of a Subprocessor by making such information available to Customer at https://trust.nuclei.ai. Customer may subscribe to receive electronic notifications of any addition or replacement of Subprocessors (which is, for the avoidance of doubt, Customer's responsibility).

7.3. Requirements for Subprocessor Engagement. When engaging any Subprocessor, Nuclei will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this DPA with respect to Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. Nuclei shall be liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

7.4. Opportunity to Object to Subprocessor Changes. When Nuclei engages any new Third-Party Subprocessor after the effective date of the Agreement, Nuclei will notify Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) by updating the Subprocessor Site or by other written means. If Customer objects to such engagement in a written notice to Nuclei within 15 days after being informed of the engagement on reasonable grounds relating to the protection of Personal Data, Customer and Nuclei will work together in good faith to find a mutually acceptable resolution to address such objection. If the Parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Services by providing written notice to Nuclei and pay Nuclei for all amounts due and owing under the Agreement as of the date of such termination.

8. Audits.

Reviews and Audits of Compliance. Customer may audit Nuclei's compliance with its obligations under this DPA, if and up to the extend needed to comply with Applicable Data Protection Laws, and up to once per year, and on such other occasions as may be required by Applicable Data Protection Laws. Nuclei will contribute to such audits by providing Customer with the information and assistance reasonably necessary to conduct the audit. If a third party is to conduct the audit, Nuclei may object to the auditor if the auditor is, in Nuclei's reasonable opinion, not independent, a competitor of Nuclei, or otherwise manifestly unsuitable. Such objection by Nuclei will require Customer to appoint another auditor or conduct the audit itself.

To request an audit, Customer must submit a proposed audit plan to Nuclei at least two weeks in advance of the proposed audit date and any third-party auditor must sign a customary non-disclosure agreement mutually acceptable to the Parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Nuclei will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Nuclei's security, privacy, employment or other relevant policies). Nuclei will work cooperatively with Customer to agree on a final audit plan.

Nothing in this Section 8 shall require Nuclei to breach any duties of confidentiality. If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2 , ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request and Nuclei has confirmed there have been no known material changes

in the controls audited since the date of such report, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures.

The audit must be conducted during regular business hours, subject to the agreed final audit plan and Nuclei's safety, security or other relevant policies, and may not unreasonably interfere with Nuclei business activities. Customer will promptly notify Nuclei of any non-compliance discovered during the course of an audit and provide Nuclei any audit reports generated in connection with any audit under this Section 8, unless prohibited by Applicable Data Protection Laws.

Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA.

Any audits are at Customer's sole expense. Customer shall reimburse Nuclei for any time expended by Nuclei and any third parties in connection with any audits or inspections under this Section 8 at Nuclei's then-current professional services rates, which shall be made available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

9. Miscellaneous.

9.1. Except as expressly modified by the DPA, the terms of the Agreement remain in full force and effect. To the extent of any conflict or inconsistency between this DPA and the other terms of the Agreement in relation to the subject matter of this DPA, this DPA will govern.

9.2. Notwithstanding anything in the Agreement or any order form entered in connection therewith to the contrary, the Parties acknowledge and agree that Nuclei's access to Personal Data does not constitute part of the consideration exchanged by the Parties in respect of the Agreement.

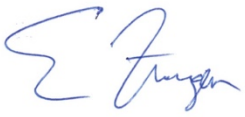
9.3. Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Nuclei to Customer under this DPA may be given (i) in accordance with any notice clause of the Agreement; (ii) to Nuclei's primary points of contact with Customer; or (iii) to any e-mail provided by Customer for the purpose of providing it with Services-related communications or alerts. Customer is solely responsible for ensuring that such e-mail addresses are valid.

9.4. Nuclei agrees to cooperate in good faith with Customer concerning any amendments as may be reasonably necessary to address compliance with the Applicable Data Protection Laws.

– signature page follows –

IN WITNESS WHEREOF, the undersigned have executed this DPA by their duly authorized representatives, with the intention to be legally bound as of the Effective Date.

NUCLEI

Signature: 

Name: Eric Franzen
Title: CEO

Address: **Nuclei, Inc.**
101 Crawfords Corner Road
Suite 4116
Holmdel, New Jersey 07757, USA

CUSTOMER

Signature: _____

Name: _____

Title: _____

_____

Address: _____

_____

_____

1. For purposes of this Annex 1, the terms "business," "commercial purpose," "sell," "share" and "service provider" shall have the respective meanings given thereto in the State Privacy Laws, and "personal information" shall mean Personal Data that constitutes personal information governed by the State Privacy Laws.

2. It is the Parties' intent that with respect to any personal information, Nuclei is a service provider. Nuclei (a) acknowledges that personal information is disclosed by Customer only for limited and specified purposes described in the Agreement; (b) shall comply with applicable obligations under the State Privacy Laws and shall provide the same level of privacy protection to personal information as is required by the State Privacy Laws; (c) agrees that Customer has the right to take reasonable and appropriate steps to help to ensure that Nuclei's use of personal information is consistent with Customer's obligations under the State Privacy Laws; (d) shall notify Customer in writing of any determination made by Nuclei that it can no longer meet its obligations under the State Privacy Laws; and (e) agrees that Customer has the right, upon notice, including pursuant to the preceding clause, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

3. Upon termination of the Agreement, Nuclei shall, at Customer's direction, delete or return all of the personal information to Customer as requested, unless retention of the personal information is required by applicable law.

4. Nuclei shall not (a) sell or share any personal information; (b) retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Services, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the Services, or as otherwise permitted by the State Privacy Laws; (c) retain, use or disclose the personal information outside of the direct business relationship between Nuclei and Customer; or (d) combine personal information received pursuant to the Agreement with personal information (i) received from or on behalf of another person, or (ii) or collected from Nuclei's own interaction with any Consumer to whom such personal information pertains, except as and to the extent necessary as a part of Nuclei's provision of the Services. Nuclei hereby certifies that it understands its respective obligations and will comply with them.

5. Giving Customer notice of Subprocessor engagements in accordance with section 7 of the DPA shall satisfy Nuclei's obligation under the State Privacy Laws to give notice of and an opportunity to object to such engagements.

6. Nuclei agrees that Company may conduct audits, in accordance with section 8 of the DPA, to help ensure that Nuclei's use of personal information is consistent with Nuclei's obligations under the State Privacy Laws.

7. The Parties acknowledge that Nuclei's retention, use and disclosure of personal information authorized by Customer's instructions documented in the DPA are integral to Vendor's provision of the Services and the business relationship between the Parties.

1. Organizational management and dedicated staff responsible for the development, implementation, and maintenance of the Nuclei's information security program.
2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Nuclei's organization, monitoring and maintaining compliance with the Nuclei's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.
3. Data security controls which include, at a minimum, logical segregation of data, restricted (e.g., role-based) access and monitoring, and utilization of commercially available industry standard encryption technologies for Personal Data that is transmitted over public networks (i.e., the Internet) or when transmitted wirelessly or at rest or stored on portable or removable media (i.e., laptop computers, CD/DVD, USB drives, back-up tapes).
4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).
5. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that the Nuclei's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on the Nuclei's computer systems; (iii) must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.
6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.
7. Physical and environmental security of data centers, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor, and log movement of persons into and out of the Nuclei's facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.
8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Nuclei's possession.
9. Change management procedures and tracking mechanisms designed to test, approve, and monitor all material changes to the Nuclei's technology and information assets.
10. Incident management procedures design to allow Nuclei to investigate, respond to, mitigate, and notify of events related to the Nuclei's technology and information assets.
11. Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
12. Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code.
13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergencies or disasters.

Detailed real-time information on Nuclei's security measures is available at: https://trust.nuclei.ai