Processor Data Processing Addendum

This Data Processing Addendum ("**DPA**") governs Company's processing of Customer Data provided by Customer to Company through Company's software-as-a-service cloud offering("**Services**") under the terms of Company's Terms of Service, Order, or other executed agreement between Customer ("**Customer**") and System Initiative, Inc. (herein, "**Company**") governing Customer's use of the Services (the "**Agreement**") and is hereby incorporated into this Agreement. If and to the extent language in this DPA conflicts with the Agreement, the conflicting terms in this DPA shall control. Capitalized terms not defined in this DPA have the meaning set forth in the Agreement.

Company and Customer each agree to comply with their respective obligations under applicable data privacy and data protection laws (collectively, "**Data Protection Laws**") in connection with the Services. Data Protection Laws may include, depending on the circumstances, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 (the California Consumer Privacy Act) ("**CCPA**"), Colo. Rev. Stat. §§ 6-1-1301 et seq. (the Colorado Privacy Act) ("**CPA**"), Connecticut's Data Privacy Act ("**CTDPA"**), Utah Code Ann. §§ 13-61-101 et seq. (the Utah Consumer Privacy Act) ("**UCPA**"), VA Code Ann. §§ 59.1-575 et seq. (the Virginia Consumer Data Protection Act) ("**VCDPA**") (collectively "**U.S. Privacy Laws**"), and the European Union General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"), and applicable subordinate legislation and regulations implementing those laws.

In connection with the Agreement, Customer is the person that determines the purposes and means for which Customer Data (as defined below) is processed (a "**Data Controller**"), whereas Company processes Customer Data in accordance with the Data Controller's instructions and on behalf of the Data Controller (as a "**Data Processor**"). "Data Controller" and "Data Processor" also mean the equivalent concepts under Data Protection Laws. For purposes of the Agreement and this DPA, (i) "**Personal Data**" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws; and (ii) "**Customer Data**" means Personal Data that Customer provides to Company that Company processes on behalf of Customer to provide the Services. Company will process Customer Data as Customer's Data Processor to provide or maintain the Services and for the purposes set forth in this DPA, the Agreement and/or in any other applicable agreements between Customer and Company.

1. **Processing Requirements.** As a Data Processor, Company agrees to:
   a. process Customer Data only (i) on Customer's behalf for the purpose of providing and supporting Company Services (including to provide insights, reporting, analytics and platform abuse, trust and safety monitoring); (ii) in compliance with the written instructions received from Customer; and (iii) in a manner that provides no less than the level of privacy protection required by Data Protection Laws;
   b. promptly inform Customer in writing if Company cannot comply with the requirements of this DPA;
   c. not provide Customer with remuneration in exchange for Customer Data from Customer;
   d. not "sell" (as such term is defined by U.S. Privacy Laws) or "share" (as such term is defined by the CCPA) Personal Data;
   e. inform Customer promptly if, in Company's reasonable opinion, an instruction from Customer violates applicable Data Protection Laws;
   f. require (i) persons employed by it and (ii) other persons engaged to perform on Company's behalf to be subject to a duty of confidentiality with respect to the Customer Data and to comply with the data protection obligations applicable to Company under the Agreement and this DPA;
   g. engage the organizations or persons listed at Exhibit https://systeminit.com/security to process Customer Data (each a "**Subprocessor**," and the list at the foregoing URL, the "**Subprocessor List**") to help Company satisfy its obligations in accordance with this DPA or to delegate all or part of the processing activities to such Subprocessors. Customer hereby consents to the use of such Subprocessors. If Customer subscribes to email notifications as provided on the Subprocessor List website, then Company will notify Customer of any changes Company intends to make to the Subprocessor List at least thirty (30) days before the changes take effect (which may be via email, a posting, or online notification for the Services or other reasonable means). In the event that Customer does not wish to consent to the use of such additional Subprocessor, Customer may notify Company that Customer does not consent within thirty (30) days on reasonable grounds relating to the protection of Customer Data by following the instructions set forth in the Subprocessor List or contacting info@systeminit.com. In such case, Company may cure the objection through one of the following options: (i) Company will cancel its plans to use the Subprocessor with regards to processing

Customer Data or will offer an alternative to provide its Services or services without such Subprocessor; (ii) Company will take the corrective steps requested by Customer in the Customer objection notice and proceed to use the Subprocessor; (iii) Company may cease to provide, or Customer may agree not to use, whether temporarily or permanently, the particular aspect or feature of the Company Services or services that would involve the use of such Subprocessor; or (iv) Customer may cease providing Customer Data to Company for processing involving such Subprocessor. If none of the above options are commercially feasible, in Company's reasonable judgment, and the objection(s) have not been resolved to the reasonable satisfaction of the parties within thirty (30) days of Company's receipt of Customer's objection notice, then either party may terminate the Services that cannot be provided without the use of the new Subprocessor for cause and in such case, Customer will be refunded any pre-paid fees for the impacted but unused Services. Such termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor. Company shall enter into contractual arrangements with each Subprocessor binding them to provide a comparable level of data protection and information security to that provided for herein. **Subject to the limitations of liability included in the Agreement, Company agrees to be liable for the acts and omissions of its Subprocessors to the same extent Company would be liable under the terms of the DPA if it performed such acts or omissions itself**;

h. upon reasonable request no more than once per year, provide Customer with Company's privacy and security policies and other information reasonably necessary to demonstrate compliance with the obligations set forth in this DPA and applicable Data Protection Laws;

i. where required by law, and upon reasonable notice and subject to appropriate confidentiality agreements, cooperate with assessments, audits, or other steps performed by or on behalf of Customer at Customer's sole expense and in a manner that is minimally disruptive to Company's business that are necessary to confirm that Company is processing Customer Data in a manner consistent with this DPA. Where permitted by law, Company may instead make available to Customer a summary of the results of a third-party audit or certification reports relevant to Company's compliance with this DPA. Such results, and/or the results of any such assessments, audits, or other steps shall be and remain the Confidential Information of Company;

j. to the extent that Customer permits or instructs Company to process Customer Data subject to U.S. Privacy Laws in a de-identified, anonymized, and/or aggregated form as part of the Services, Company shall: (i) adopt reasonable measures to prevent such de-identified data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (ii) not attempt to re-identify the information, except that Company may attempt to re-identify the information solely for the purpose of determining whether its de-identification processes comply with Data Protection Laws or are functioning as intended; and (iii) before sharing de-identified data with any other party, including Subprocessors, contractually obligate any such recipients to comply with the requirements substantially similar to this provision;

k. where the Customer Data is subject to the CCPA, not (i) retain, use, disclose, or otherwise process Customer Data except as necessary for the business purposes specified in the Agreement or this DPA; (ii) retain, use, disclose, or otherwise process Customer Data in any manner outside of the direct business relationship between Company and Customer; or (iii) combine any Customer Data with Personal Data that Company receives from or on behalf of any other third party or collects from Company's own interactions with individuals, provided that Company may so combine Customer Data for a purpose permitted under the CCPA if directed to do so by Customer or as otherwise permitted by the CCPA;

l. where required by law, grant Customer the rights to (i) take reasonable and appropriate steps to ensure that Company uses Customer Data in a manner consistent with Data Protection Laws by exercising the audit provisions set forth in this DPA; and (ii) stop and remediate unauthorized use of Customer Data.

2. **Notice to Customer.** Company will inform Customer if Company becomes aware of: (a) any legally binding request for disclosure of Customer Data by a law enforcement authority, unless Company is otherwise forbidden by law to inform Customer; (b) any notice, inquiry or investigation by an independent public authority established by a member state pursuant to Article 51 of the GDPR (a "**Supervisory Authority**") with respect to Customer Data; or (c) any complaint or request (in particular, requests for access to, rectification or blocking of Customer Data) received directly from Customer's data subjects. Company will not respond to any such request without Customer's prior written authorization.

3. **Assistance to Customer.** Company will provide reasonable assistance to Customer regarding:

   a. information necessary, taking into account the nature of the processing, to respond to valid requests received pursuant to Data Protection Laws from Customer's data subjects in respect of access to or the rectification, erasure, restriction, portability, objection, blocking or deletion of Customer Data that

Company processes for Customer. In the event that a data subject sends such request directly to Company, Company will promptly send such request to Customer;

b. the investigation of any breach of Company's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Data processed by Company for Customer (a "**Personal Data Breach**"); and

c. where appropriate, the preparation of data protection impact assessments with respect to the processing of Customer Data by Company and, where necessary, carrying out consultations with any supervisory authority with jurisdiction over such processing.

4. **Required Processing.** If Company is required by Data Protection Laws to process any Customer Data for a reason other than in connection with the Agreement, Company will inform Customer of this requirement in advance of any such processing, unless legally prohibited to do so.

5. **Security.** Company will:

a. maintain reasonable and appropriate organizational and technical security measures to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer Data and to protect the rights of the subjects of that Customer Data;

b. take appropriate steps to confirm that Company personnel are protecting the security, privacy and confidentiality of Customer Data consistent with the requirements of this DPA; and

c. notify Customer of any Personal Data Breach by Company, its Subprocessor, or any other third parties acting on Company's behalf without undue delay after Company becomes aware of such Personal Data Breach.

6. **Obligations of Customer.**

a. Customer represents, warrants and covenants that it has and shall maintain throughout the term all necessary rights, consents and authorizations to provide the Customer Data to Company and to authorize Company to use, disclose, retain and otherwise process Customer Data as contemplated by this DPA, the Agreement and/or other processing instructions provided to Company.

b. Customer shall comply with all applicable Data Protection Laws.

c. Customer shall reasonably cooperate with Company to assist Company in performing any of its obligations with regard to any requests from Customer's data subjects.

d. Without prejudice to Company's security obligations in Section 5 of this DPA, Customer acknowledges and agrees that it is responsible for certain configurations and design decisions for the services and that Customer is responsible for implementing those configurations and design decisions in a secure manner that complies with applicable Data Protection Laws.

e. Customer shall not provide Customer Data to Company except through agreed mechanisms. Without limitation to the foregoing, Customer represents, warrants and covenants that it shall only transfer Customer Data to Company using secure, reasonable and appropriate mechanisms, to the extent such mechanisms are within Customer's control.

f. Customer shall not take any action that would (i) render the provision of Customer Data to Company a "sale" under U.S. Privacy Laws or a "share" under the CCPA (or equivalent concepts under U.S. Privacy Laws); or (ii) render Company not a "service provider" under the CCPA or "processor" under U.S. Privacy Laws.

7. **Standard Contractual Clauses.**

a. Company will process Customer Data that originates in the European Economic Area in accordance with the standard contractual clauses adopted by the EU Commission on June 4, 2021 ("**EU SCCs**") which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

i. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Company is processing Customer Data as a processor.

ii. Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Company is processing Customer Data as a sub-processor.

b. For each module of the EU SCCs, where applicable, the following applies:

i. The optional docking clause in Clause 7 does not apply;

ii. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 1(g) of this DPA.

iii. In Clause 11, the optional language does not apply;

iv. All square brackets in Clause 13 are hereby removed;

v. In Clause 17 (Option 1), the EU SCCs will be governed by the EU member state where the data exporter is located;

vi. In Clause 18(b), disputes will be resolved before the courts of the EU member state where the data exporter is located;

vii. Exhibit A to this DPA contains the information required in Annex I and Annex III of the EU SCCs;

viii. Exhibit B to this DPA contains the information required in Annex II of the EU SCCs; and

c. Customer Data originating from Switzerland shall be processed in accordance with the EU SCCs with the following amendments:

i. "FDPIC" means the Swiss Federal Data Protection and Information Commissioner. ii. "Revised FADP" means the revised version of the FADP of 25 September 2020, which is scheduled to come into force on 1 January 2023.

iii. The term "EU Member State" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).

iv. The EU SCCs also protect the data of legal entities until the entry into force of the Revised FADP.

v. The FDPIC shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP

d. With respect to Customer Data originating from the United Kingdom, the parties will comply with the terms of Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses (the "**UK Addendum**"). The parties also agree (i) that the information included in Part 1 of the UK Addendum is as set out in Annex I of Appendix A to this DPA and (ii) that either party may end the UK Addendum as set out in Section 19 of the UK Addendum.

8. **Term; Data Return and Deletion.** This DPA shall remain in effect as long as Company carries out Customer Data processing operations on Customer's behalf or until the termination of the Agreement (and all Customer Data has been returned or deleted in accordance with this DPA). Company will retain Customer Data sent through the API for a maximum of thirty (30) days, after which it will be deleted, except where Company is required to retain copies under applicable laws, in which case Company will isolate and protect that Customer Data from any further processing except to the extent required by applicable laws. On the termination of the DPA, Company will direct each Subprocessor to delete the Customer Data within thirty (30) days of the DPA's termination, unless prohibited by law. For clarity, Company may continue to process information derived from Customer Data that has been deidentified, anonymized, and/or aggregated such that the data is no longer considered Personal Data under applicable Data Protection Laws and in a manner that does not identify individuals or Customer to improve Company's systems and services.

System Initiative, Inc. (Company)	**Customer**
Signature:	Signature:
Name:	Name:
Title: Authorized Signer	Title:
Date:	Date:

Exhibit A

ANNEX I

DETAILS OF PROCESSING

A. LIST OF PARTIES

Name of Data Importer:	The party identified as the "Company" in this DPA
Address:	548 Market St Ste 66061 San Francisco, CA, 94104-5401
Contact person's name, position, and contact details:	Will be provided upon request.
Activities relevant to the data transferred under these Clauses:	See Annex 1(B) below and the Agreement.
Signature and date:	This Annex I shall automatically be deemed executed when the DPA is executed by Company.
Role (controller/processor):	Processor

Name of Data Exporter:	The party identified as the "Customer" in this DPA.
Address:	Reference is made to the Agreement.
Contact person's name, position, and contact details:	Reference is made to the Agreement.
Activities relevant to the data transferred under these Clauses:	See Annex 1(B) below and the Agreement.
Signature and date:	This Annex I shall automatically be deemed executed when the DPA is executed by Customer.
Role (controller/processor):	Controller

B. DESCRIPTION OF PROCESSING/ TRANSFER

Categories of Data Subjects whose Personal Data is transferred	The Data Subjects whose Personal Data is Processed by Company when providing the Services to Customer.
Categories of Personal Data transferred	The categories of Personal Data that is Processed by Company when providing the Services to Customer.
Sensitive data transferred (if applicable) and applied restrictions or safeguards	No sensitive data is processed under the Agreement.
Frequency of Transfer	Continuous.
Nature and purpose(s) of the data transfer and Processing	Company will process Personal Data as necessary to provide the Services under the Agreement, including the provision of an API to engage users, power cross-channel workflows, and manage notification preferences.
Retention period (or, if not possible to determine, the criterial used to deter- mine the period)	Personal Data will be retained for as long as necessary taking into account the purpose of the Processing, and in compliance with applicable laws, including laws on the statute of limitations and Data Protection Law.
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing	Company will restrict the onward Subprocessor's access to Customer Personal Data only to what is strictly necessary to provide the Services, and Company will prohibit the Subprocessor from Processing the Customer Personal Data for any other purpose.
Identify the competent supervisory authority/ies in accordance with Clause 13	Where the EU GDPR applies, the competent authority will be determined in accordance with Clause 13 of the Standard Contractual Clauses. Where the UK GDPR applies, the UK Information Commissioner's Office.

Exhibit B

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES

INTRODUCTION

Company's mission is to deploy safe and responsible services at scale for the benefit of all. In accordance with this mission, Company maintains an information security program designed to safeguard its systems, data, and Customer Data. This Addendum describes the information security program and security standards that Company maintains with respect to the Services and handling of data submitted by or on behalf of Customer for the Services (the "Customer Data"). Capitalized terms not defined in this Annex II have the meanings given in the DPA or Agreement.

To learn more about Processor's technical and organizational security measures to protect Customer Data, see the Company Security Description at https://systeminit.com/security (the "Security Portal"). The Security Measures below include the subset of the information available in the Security Portal which applies to this DPA.

SECURITY MEASURES

1. Security Management	System Initiative utilizes Amazon Web Services (AWS) as its cloud service provider. AWS's security and compliance controls are employed to manage data center physical security and cloud infrastructure security. These controls are designed to safeguard data against unauthorized access and meet industry standards for security and compliance. Access to platforms containing Personally Identifiable Information (PII) by System Initiative employees is currently managed through Google-based Single Sign-On (SSO). This approach ensures centralized access control and strengthens authentication processes. Additional information on AWS security measures is available on the AWS Security Cloud website.
2. Maintaining of an Information Security Policy	System Initiative maintains an Information Security Policy that includes incident response protocols and response categorization standards. The policy encompasses procedures for identifying, responding to, and mitigating security incidents, ensuring that appropriate actions are taken based on the severity and impact of the incident. System Initiative employs monitoring and alerting tools, such as Grafana, CloudWatch, and Honeycomb, to oversee production environments and detect potential security events. Role-Based Access Control (RBAC) is implemented across all services to manage user access to AWS and other resources, ensuring that access rights are appropriately assigned based on job roles and

	responsibilities. AWS CloudTrail is utilized to provide API-level change control across all environments, enabling comprehensive auditing and tracking of API activity to maintain accountability and transparency in the management of cloud resources.
3. Secure Networks and Systems	System Initiative employs AWS Virtual Private Cloud (VPC) to ensure secure networking and system architecture. Network isolation is strictly enforced between services that do not require direct routing, between different environments, and between local users and services, to minimize unauthorized access and minimize attack surfaces. Changes to networking rules and services are managed through controlled processes within System Initiative, ensuring that upgrades and modifications are subject to review and approval procedures to maintain the integrity and security of network configurations.
4. **Personal Data Protection Measures (including storage limitation, data minimization and retention and encryption)**	System Initiative implements various measures to protect personal data, including encryption, access control, and key management. Personally Identifiable Information (PII) is universally encrypted at rest and in transit across all stages of its lifecycle within the SI environments. This may vary for data movements and storage within third party processors. HTTPS is utilized for data transmission into the authentication portal, and all public network connections are similarly protected to ensure secure data transfer. PII Data will be retained for a maximum of 4 years after last activity, to allow System Initiative to comply with specific governmental and compliance requirements. Retention on specific database and service backups will vary depending on various operational factors. Sensitive values within each workspace within System Initiative are secured with unique cryptographic keys. These keys are securely stored and managed within AWS Secrets Manager. System Initiative employs encryption for data at rest and secures network communication using TLS for data in transit, thereby maintaining robust encryption standards. ** Workspaces being a level of tenancy within the System Initiative Product*
5. Vulnerability Management Efforts	System Initiative employs a comprehensive approach to vulnerability management to ensure the security and integrity of its software. Code is scanned daily for Common Vulnerabilities and Exposures (CVEs) using GitHub's integrated security tools. While we are an open-source platform and cannot guarantee

	endpoint protection for community-provided code, each contribution is individually reviewed, tested, and subjected to thorough analysis before being merged into the main trunk of the repository. System Initiative utilizes isolated environments at multiple stages of the Software Development Lifecycle (SDLC), with strict segregation between production and testing environments. Continuous integration and delivery processes are facilitated through Buildkite, our CI tooling. Every pull request (PR) merged into our codebase undergoes a rigorous pipeline of automated tests and security analysis appropriate to the nature of the code, irrespective of its source. Our testing framework includes robust unit and integration testing to identify and mitigate vulnerabilities proactively, ensuring that our software maintains high standards of security and reliability throughout its lifecycle.
6. Access Control Measures	System Initiative implements a zero-trust access model across all systems, where users, service accounts, and role assumptions are denied access by default and must be explicitly granted permissions. Access to all components of our infrastructure and product stack requires Multi-Factor Authentication (MFA), and user permissions are strictly aligned with their designated roles. Expired or terminated users are removed from the system within 30 days, and the use of static credentials is minimized wherever feasible. System Initiative ensures that all actions performed by users within the AWS production environment are logged through comprehensive Audit Logs, providing full traceability of user activities. All users are required to adhere to industry-standard password complexity requirements, which are enforced through G Suite Single Sign-On (SSO). Access to System Initiative products and customer data is restricted to a limited subset of personnel, who access these resources through controlled interfaces. This restricted access is intended to facilitate effective customer support, troubleshoot issues, respond to security incidents, and maintain data security.
7. Restriction of Physical Access to Personal Data Processing Systems	System Initiative relies primarily on Amazon Web Services (AWS) and , in the future, other vetted cloud providers for hosting and processing personal data, thereby adhering to the stringent physical security measures established by these providers. These measures include robust access controls, surveillance, and other physical security protocols designed to protect data processing systems from unauthorized access.

8. Regular Monitoring and Testing of Networks	As System Initiative operates without physical offices or on-premises networks, traditional office and building security measures are not applicable. However, we maintain a strong focus on securing our virtual environments. System Initiative conducts regular penetration testing on its production environment and associated services to identify and address potential vulnerabilities. These tests are performed on a recurring basis to ensure that our network defenses remain robust and responsive to evolving security threats.
9. Incident Response Plan	System Initiative has an established Incident Response Plan that utilizes industry-standard tools, including FireHydrant, for effective incident management. Our response strategy includes 24/7 on-call personnel to ensure prompt reaction to incidents as they arise. We maintain specific runbooks tailored to handle various types of incidents, providing structured guidance for incident resolution. Communication during incidents is facilitated through multiple channels, including a public status page, RSS feeds, and direct communication methods where appropriate, to keep stakeholders informed. System Initiative also maintains comprehensive database backup and recovery procedures, with structured methods in place to handle data restoration, reparation and service continuity during incidents.
10. Third Party Risk Management Program	System Initiative ensures that all third-party providers used in our customer operations meet stringent security standards, including at least SOC 2 Type 2 compliance. We consistently perform due diligence to assess and select vendors based on their security practices and compliance with industry standards. Discord, while utilized, consuming PII from users themselves and acting as a cornerstone of the System Initiative community is not a mandatory component of our vendor ecosystem and Slack will be used where customers require stricter compliance for vendors.