DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") governs processing of Customer Data provided by Customer to SFive Inc. d.b.a Iudex through Iudex's hosted software solution (the "Service") pursuant to Iudex' terms of service ("ToS") or any other commercial agreement (the "Agreement") which supersedes the ToS and governs the use of the Service by Customer. If and to the extent language in this DPA conflicts with the ToS or 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. For the purposes of this DPA only, "Customer" includes any affiliate entity of Customer's that (a) is using the Service pursuant to the rights obtained by it or its Affiliate, and that (b) directly or indirectly, through one or more intermediaries controls, is controlled by, or is under common control with Customer.

In addition to anything set out under the Agreement and the ToS, Iudex 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 United Kingdom and/or European Union General Data Protection Regulation (Regulation (EU) 2016/679) (collectively the "GDPR"), and applicable subordinate legislation and regulations implementing those laws.

In connection with the ToS and 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 Iudex processes Customer Data in accordance with the Data Controller's commands 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 the 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 Iudex that Iudex processes on behalf of Customer to provide the Services. Iudex 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 ToS and/or the Agreement between Customer and Iudex.

1. Processing Requirements

As a Data Processor, Iudex agrees to:

a. process Customer Data only (i) on Customer's behalf for the purpose of providing and supporting Iudex's Services (including to provide insights, reporting and analytics); (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 of it by Data Protection Laws;

b. promptly inform Customer in writing if Iudex cannot comply with the requirements of this DPA;

c. not provide Customer with remuneration in exchange for Customer Data from Customer. The parties acknowledge and agree that Customer has not "sold" (as such term is defined by the CCPA) Customer Data to Iudex;

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 Iudex's 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 Iudex'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 Iudex under the Agreement and this DPA;

g. engage the organizations or persons listed at https://appplatform.iudex.com/subprocessors

to process Customer Data (each "Subprocessor," and the list at the foregoing URL, the "Subprocessor List") to help Iudex 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 Iudex will notify Customer of any changes Iudex intends to make to the Subprocessor List at least 15 days before the changes take effect (which may be via email, a posting, or notification on an online portal for our 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 Iudex that Customer does not consent within fifteen (15) days on reasonable grounds relating to the protection of Customer Data by following the instructions set forth in the Subprocessor List or by contacting privacy@iudex.com. In such case, Iudex shall have the right to cure the objection through one of the following options: (i) Iudex 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) Iudex will take the corrective steps requested by Customer in Customer objection notice and proceed to use the Subprocessor; (iii) Iudex may cease to provide, or Customer may agree not to use whether temporarily or permanently, the particular aspect or feature of the Iudex Services or services that would involve the use of such Subprocessor; or (iv) Customer may cease providing Customer Data to Iudex for processing involving such Subprocessor. If none of the above options are commercially feasible, in Iudex's reasonable judgment, and the objection(s) have not been resolved to the satisfaction of the parties within thirty (30) days of Iudex's receipt of Customer's objection notice, then either party may terminate any subscriptions, order forms or usage regarding 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 applicable subscriptions, order forms or usage to the extent they cover periods or terms following the date of such termination. Such termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor. Iudex 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, Iudex agrees to be liable for the acts and omissions of its Subprocessors to the same extent Iudex 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 Iudex's privacy and security policies and other such information 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 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 Iudex's business that are necessary to confirm that Iudex is processing Customer Data in a manner consistent with this DPA. Where permitted by law, Iudex may instead make available to Customer a summary of the results of a third-party audit or certification reports relevant to Iudex's compliance with this DPA. Such results, and/or the results of any such assessments, audits, or other steps shall be the Confidential Information of Iudex;

j. to the extent that Customer permits or instructs Iudex to process Customer Data subject to U.S. Privacy Laws in a de-identified, anonymized, and/or aggregated form as part of the Services, Iudex shall (i) adopt reasonable measures to prevent such deidentified 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 Iudex may attempt to reidentify 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 of 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 Iudex and Customer; or (iii) combine any Customer Data with Personal Data that Iudex receives from or on behalf of any other third party or collects from Iudex's own interactions with individuals, provided that Iudex 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 Iudex uses Customer Data in a manner consistent with Data Protection Laws by exercising the audit provisions set forth in this DPA above; and (ii) stop and remediate unauthorized use of Customer Data, for example by requesting that Iudex provide written confirmation that applicable Customer Data has been deleted.

2. Notice to Customer

Iudex will inform Customer if Iudex becomes aware of:

a. any legally binding request for disclosure of Customer Data by a law enforcement authority, unless Iudex is otherwise forbidden by law to inform Customer, for example to preserve the confidentiality of an investigation by law enforcement authorities;

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. Iudex will not respond to any such request without Customer's prior written authorization.

3. Assistance to Customer

Iudex will provide reasonable assistance to Customer regarding, as applicable:

a. information necessary, taking into account the nature of the processing, to respond to 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 Iudex processes for Customer. In the event that a data subject sends such a request directly to Iudex, Iudex will promptly send such request to Customer;

b. the investigation of any breach of Iudex's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Data processed by Iudex 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 Iudex and, where necessary, carrying out consultations with any supervisory authority with jurisdiction over such processing.

4. Required Processing

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

5. Security

Iudex will:

a. maintain reasonable and appropriate organizational and technical security measures, including but not limited to those measures described in Exhibit A to this DPA (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, and encryption) 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 Iudex 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 Iudex, its Subprocessors, or any other third parties acting on Iudex's behalf without undue delay after Iudex 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 Iudex and to authorize Iudex to use, disclose, retain and otherwise process Customer Data as contemplated by this DPA, the Agreement and/or other processing instructions provided to Iudex.

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

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

d. Without prejudice to Iudex's security obligations in Section 5 of this DPA, Customer acknowledges and agrees that it, rather than Iudex, is responsible for certain configurations and design decisions for the services and that Customer, and not Iudex, 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 Iudex except through agreed mechanisms. For example, Customer shall not include Customer Data other than technical contact information, or in technical support tickets, transmit user Customer Data to Iudex by email. Without limitation to the foregoing, Customer represents, warrants and covenants that it shall only transfer Customer Data to Iudex 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 Iudex a "sale" under U.S. Privacy Laws or a "share" under the CCPA (or equivalent concepts under U.S. Privacy Laws); or (ii) render Iudex not a "service provider" under the CCPA or "processor" under U.S. Privacy Laws.

8. Term; Data Return and Deletion

This DPA shall remain in effect as long as Iudex 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). On the termination of the DPA, Iudex will direct each Subprocessor to delete the Customer Data within thirty (30) days of the DPA's termination, unless prohibited by law. For clarity, Iudex 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 Iudex's systems and services.

Exhibit A
TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

SECURITY MEASURES

Corporate Identity, Authentication, and Authorization Controls. Iudex maintains industry best practices for authenticating and authorizing internal employee and service access, including the following measures:

- Iudex uses single sign-on (SSO) to authenticate to third-party services used in the delivery of the Services. Role Based Access Controls (RBAC) are used when provisioning internal access to the Services;
- Mandatory multi-factor authentication is used for authenticating to Iudex's identity provider;
- Unique login identifiers are assigned to each user;
- Established review and approval processes for any access requests to services storing Customer Data;
- Periodic access audits designed to ensure access levels are appropriate for the roles each user performs;
- Established procedures for promptly revoking access rights upon employee separation;

- Established procedures for reporting and revoking compromised credentials (such as passwords and API keys); and
- Established password reset procedures, including procedures designed to verify the identity of a user prior to a new, replacement, or temporary password.

Customer Identity, Authentication, and Authorization Controls. Iudex maintains industry best practices for authenticating and authorizing customers to the Services, including the following measures:

- Use of a third-party identity access management service to manage Customer identity, meaning Iudex does not store user-provided passwords on users' behalf; and
- Logically separating Customer Data by organization account using unique identifiers. Within an organization account, unique user accounts are supported.
- Cloud Infrastructure and Network Security. Iudex maintains industry best practices for securing and operating its cloud infrastructure, including the following measures:
- Separate production and non-production environments;
- Primary backend resources are deployed behind a VPN;
- The Services are routinely audited for security vulnerabilities;
- Application secrets and service accounts are managed by a secrets management service;
- Network security policies and firewalls are configured for least-privilege access against a pre-established set of permissible traffic flows. Non-permitted traffic flows are blocked; and
- Services logs are monitored for security and availability.

Data Access Control. Iudex maintains industry best practices for preventing authorized users from accessing data beyond their authorized access rights and for preventing the unauthorized input, reading, copying, removal, modification, or disclosure of data. Such measures include the following:

- Employee access to the Services follows the principle of least privilege. Only employees whose job function involves supporting the delivery of Services are credentialed to the Services environment; and
- Customer Data submitted to the Services is only used in accordance with the terms of the DPA, Agreement, and any other applicable contractual agreements in place with Customer.

Disclosure Control. Iudex maintains industry best practices for preventing the unauthorized access, alteration, or removal of data during transfer, and for securing and logging all transfers. Such measures include:

- Encryption of data at rest in production datastores using strong encryption algorithms;
- Encryption of data in transit;
- Audit trail for all data access requests for production datastores;
- Full-disk encryption required on all corporate workstations;
- Device management controls required on all corporate workstations;
- Restrictions on use of portable or removable media; and

- Customer Data can be deleted upon request.

Availability Control. Iudex maintains industry best practices for maintaining Services functionality through accidental or malicious intent, including:

- Ensuring that systems may be restored in the event of an interruption;
- Ensuring that systems are functioning and faults are reported; and
- Anti-malware and intrusion detection/prevention solutions implemented comprehensively across our environment.

Segregation Control. Iudex maintains industry best practices for separate processing of data collected for different purposes, including:

- Logical segregation of Customer Data;
- Restriction of access to data stored for different purposes according to staff roles and responsibilities;
- Segregation of business information system functions; and
- Segregation of testing and production information system environments.

Third Party Risk Management. Iudex maintains industry best practices for managing third party security risks, including with respect to any subprocessor or subcontractor to whom Iudex provides Customer Data, including the following measures:

- Written contracts designed to ensure that any agent agrees to maintain reasonable and appropriate safeguards to protect Customer Data

Security Incident Response. Iudex maintains a security incident response plan for responding to and resolving events that compromise the confidentiality, availability, or integrity of the Services or Customer Data including the following:

- Iudex aggregates system logs for security and general observability from a range of systems to facilitate detection and response; and
- If Iudex becomes aware that a Personal Data Breach has occurred, Iudex will notify Customer in accordance with the DPA.

Security Evaluations. Iudex performs regular security and vulnerability testing to assess whether key controls are implemented properly and are effective as measured against industry security standards and

its policies and procedures and to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the security of Customer Data as well as the maintenance and structure of Iudex's information systems.