

## Standard Terms of Service

These Standard Terms of Service are the terms and conditions pursuant to which TokenEx will deliver its services to any client. There is an addendum to this document which deals with GDPR, and which may supplement these terms and conditions if necessary, and to the extent applicable.

### Definitions:

“Affiliates” means any entities that a party directly or indirectly controls, is controlled by or is under control of that party.

“Availability” means the time in which the Client is able to connect to and transfer data with the System on a monthly basis, excluding Scheduled Maintenance and Emergency Security Updates.

“Client” is any person or entity that uses TokenEx’s services to improve data security. For example, a Client could be someone that uses TokenEx to secure data within Client’s own corporate environment, or a Client who uses TokenEx’s services within Client’s product offering to secure Client’s customer data.

“Emergency Security Update” means a period for which the Services are unavailable for use by Client in order to perform emergency security updates or perform similar work, and for which Client has been given prior notice of such period.

“Platform Credentials” means all credentials provided or related to accessing the TokenEx Platform. TokenEx shall provide Client with Platform Credentials, including but not limited to (1) API Keys, (2), SFTP user accounts and (3) customer portal user accounts.

“Quote for Services” means “Exhibit B”, as attached to the final contractual document. The Quote for Services will contain the details of pricing and specific services provided to Client.

“Service Level Agreement” means “Exhibit A” as attached to the final contractual document. The Service Level Agreement will contain proprietary details about availability uptimes, response times, and other related information.

“Scheduled Maintenance” means a period for which the Services are scheduled to be unavailable for use by Client in order to perform preventive maintenance, install upgrades or perform similar work, and for which Client has been given prior notice of such period.

“TokenEx Platform” means the software products owned or licensed by TokenEx to which TokenEx grants Client access as part of the services, including, but not limited to (1) Web API's, (2) Hosted payment pages/iframe, (3) batch file processing (sftp) and (4) customer portal.

“Whitelisting” is a process which checks connecting IP addresses against an approved list of IP addresses (“Approved IPs”) that Client submits to be open and accessible. Only those “Approved IPs” will be granted access to the TokenEx platform.

**1. Provision of Services.** TokenEx, LLC (“TokenEx”) shall provide services to Client (identified in the signature block hereof) and Client shall pay for such services in accordance with the terms of this Service Agreement (“Agreement”) and the Quote for Services attached hereto during the initial subscription term and any extension thereof. This Agreement will automatically renew following each contract year, but

may be terminated by either party upon providing the other party not less than thirty (30) days prior written notice of any termination. Client shall be obligated to pay any and all outstanding charges for services that have been delivered or invoiced prior to the date of termination.

2. TokenEx Responsibilities. TokenEx shall also provide basic support for the services at no additional charge, and use all reasonable, good-faith efforts to provide the services 24 hours a day, 7 days a week, except for (a) Scheduled Maintenance following at least five (5) days advance notice to Client, (b) any Emergency Security Update, for which TokenEx shall give notice by email as promptly as reasonably practicable, or (c) any unavailability caused by circumstances beyond TokenEx's reasonable control. TokenEx has and will maintain during the Term, at least the following certifications: PCI-DSS Level 1 Service Provider, Privacy Shield (EU-US and Swiss-US), and SSAE 16 SOC 2 Type II.

Protection of Data. TokenEx shall maintain administrative, physical, and technical safeguards for protection of Client's data. TokenEx shall not modify Client's data or access it except to prevent or address service problems.

Privacy Rules. TokenEx shall comply with all applicable privacy laws and regulations to the extent that those laws apply to the services being performed under this Agreement. In the event that a governmental authority or other authority having jurisdiction requests that all or any part of Client's data be disclosed, TokenEx shall, if allowed by law, within two (2) business days inform Client of the request or subpoena, and cooperate with Client in any defense Client wishes to make to the request or subpoena, at Client's expense.

Background Checks. TokenEx shall perform background checks on all employees involved in the performance of services to Client, including, at a minimum: SSN verification (with trace), academic credentials (highest level of education earned or most recent place of attendance), employment history (all employers for the longer of last seven years or last three employers), Domestic Terror Watchlist and criminal history (all felonies, misdemeanors, convictions, current indictments, and time served for last seven years in all counties of residence).

3. Client Responsibilities. Client shall be responsible for the accuracy, quality and content of all of Client's data subject to this Agreement, and use commercially reasonable efforts to prevent unauthorized access to or use of the services. Client agrees to promptly notify TokenEx of any unauthorized access or use, and use the services in compliance with all applicable laws and government regulations. Client agrees not to make TokenEx's services available to any third party, or to sell, resell, rent or lease the Services, unless pursuant to a separate negotiated agreement with TokenEx, or as a value-added service incorporated into Client's product offering, and then with prior notification to and prior written permission of TokenEx. Client further agrees not to use production data within the TokenEx test environment.

4. TokenEx Platform Credentials.

TokenEx shall provide Client with Platform Credentials, including but not limited to (1) API Keys, (2), SFTP user accounts and (3) customer portal user accounts. **Platform Credentials are SOLELY and exclusively for the use of Client. Notwithstanding any other provision in this Agreement, Client agrees that in the event Client provides or discloses Platform Credentials to any third party, Client is liable for any harm, injury or damages whatsoever arising from any such disclosure.**

In the event Client discloses TokenEx's Platform Credentials to any party other than Client's employees, contractors, and outsourcers performing services for or on behalf of Client, Client understands

and agrees that TokenEx disclaims any and all liability or responsibility whatsoever for any breach, disclosure or loss of Client data. By disclosing TokenEx's Platform Credentials in breach of this Agreement, Client understands that Client is exposing Client's data vault contents to breach, and that Client assumes any and all liability whatsoever for any breach of Client's data vault.

Additionally, and in addition to the foregoing complete release of any and all liability, Client assumes any and all risks incident to the disclosure by Client (including any of Client's employees, officers or directors) of Client's Platform Credentials. Client hereby releases and holds TokenEx harmless from any and all liability of any kind or character whatsoever, in any form or forum, and to the fullest extent available under applicable law, concerning, arising from or in any way related to damages that Client may sustain following Client's disclosure of TokenEx's Platform Credentials.

5. Whitelisting. TokenEx, as part of its authentication model, employs IP Whitelisting. In the event Client elects not to utilize the Whitelisting service TokenEx provides as part of the TokenEx authentication model, then TokenEx disclaims any and all liability or responsibility whatsoever for any breach of Client's data. By electing not to use TokenEx's IP address validation component of TokenEx's authorization model, Client understands that Client is exposing Client's data vault contents to breach. Client hereby releases and holds TokenEx harmless from any and all liability of any kind or character whatsoever, in any form or forum, and to the fullest extent available under the applicable law, concerning, arising from, or in any way related to damages that Client may sustain as a result of an unauthorized disclosure of Client's data which was not a direct result of TokenEx's breach of any of its obligations hereunder.

6. Fees, Invoicing and Payment. Client agrees to pay the fees set forth in the Quote for Services, to be attached to the final contractual document. Client may pay for the services with a credit card and authorize TokenEx to charge such credit card for all fees related to this Agreement. If the order form specifies that payment may be by a method other than a credit card, TokenEx will invoice Client. Invoiced charges are due net thirty (30) days from the invoice date.

7. Warranties. TokenEx warrants (1) that the Services will perform as designed, (2) that the functionality of the Services will not be materially decreased, and (3) that TokenEx will perform the Services described herein in a professional manner consistent with industry standards and this Agreement.

8. Indemnification. Each party ("Indemnifying Party") shall, to the extent caused by the indemnifying party's negligent act or omission, defend, indemnify and hold harmless the other party, its Affiliates and their respective directors, shareholders, employees and officers (collectively, "Indemnified Parties") from and against all claims, losses, liabilities (including negligence, tort and strict liability), damages, judgments, suits and all legal proceedings, and any and all costs and expenses in connection therewith (including any interest, penalties, fines and reasonable legal fees and disbursements) (individually, a "Claim" or collectively, "Claims") arising out of or in any manner connected with any breach of any representation, warranty, covenant or other obligation of the Indemnifying Party contained herein. A party seeking indemnity from the other party shall promptly notify the other party of any Claim and shall provide information, assistance and cooperation in defending against such Claim at the Indemnifying Party's sole cost and expense. Any such notification shall be in writing and directed to the person designated in the "Notification" paragraph hereof. In addition, an Indemnified Party shall have the right to participate in the defense of any Claim, suit or proceeding at its own sole cost and expense.

The right to indemnity provided for in this paragraph is subject to the non-breaching party's notification to the alleged breaching party of any known breach of the provisions hereof, and providing

the alleged breaching party with a reasonable time within which to correct the alleged breach, and provide evidence of any such correction. The right to correct a breach provided for herein shall not apply to the Nondisclosure provisions of this Agreement.

9. Limitation of Liability. THIS PARAGRAPH DOES NOT APPLY TO ANY OBLIGATIONS ARISING UNDER THE NONDISCLOSURE SECTION(S) OF THIS AGREEMENT (for example, a data breach or any disclosure of confidential information would not be subject to this paragraph). EXCEPT FOR OBLIGATIONS ARISING UNDER THE NONDISCLOSURE PROVISIONS, NEITHER PARTY'S LIABILITY WITH RESPECT TO ANY SINGLE INCIDENT ARISING OUT OF OR RELATED TO THIS AGREEMENT (WHETHER IN CONTRACT OR TORT OR UNDER ANY OTHER THEORY OF LIABILITY) SHALL EXCEED THE AMOUNT PAID BY CLIENT HEREUNDER IN THE 12 MONTHS PRECEDING THE INCIDENT, PROVIDED THAT IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT (WHETHER IN CONTRACT OR TORT OR UNDER ANY OTHER THEORY OF LIABILITY) EXCEED THE TOTAL AMOUNT PAID BY CLIENT HEREUNDER. THE FOREGOING SHALL NOT LIMIT CLIENT'S PAYMENT OBLIGATIONS. IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY FOR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

10. Prices. Pricing reflected on the attached Quote for Services is firm for the subscription term indicated. Any pricing modification(s) under this Agreement on any renewal thereof shall not exceed five (5) percent from the prior term except by written agreement of the parties.

11. Insurance. TokenEx shall maintain, at TokenEx's own expense and in reasonable amounts acceptable to Client, professional liability insurance covering the effects of errors and omissions in the performance of professional duties, including cyber liability and network security coverage, with coverage limits of not less than \$5,000,000 per claim. Upon request, Client shall be named as an additional insured as Client's interests may appear on liability policies. A Certificate of Liability Insurance shall be furnished to Client upon request following the execution of this Agreement.

12. Return of Data/Notice. Client may request the return of Client's stored data in the possession or control of TokenEx at the end of a subscription term, or upon termination of this Agreement or any extension or renewal hereof. Any request must be in writing and received by TokenEx within thirty (30) days following the effective date of termination. Thereafter, TokenEx shall have no further legal or business obligation to maintain or provide any of the data after that time and all such data shall be deleted from TokenEx's systems. Stored data shall be returned to Client not later than fourteen (14) days following receipt of a written request.

13. Applicable Law. In any dispute arising under this Agreement, the laws of the State of Delaware shall govern without regard to the choice of law rules of any jurisdiction, including Delaware.

14. Arbitration. Any controversy, dispute or claim arising out of, in connection with, or in relation to, the interpretation, performance or breach of this Agreement, including, without limitation, the validity, scope and enforceability of this Agreement, that is not first resolved by negotiation between the parties, shall be submitted to binding and final arbitration by a single arbitrator selected by the American Arbitration Association ("AAA"), having experience in data security, and conducted pursuant to the rules of the AAA. Any such action or claim must be brought within two (2) years of the date the claim arose. The arbitrator shall be limited solely to awarding remedies that are permitted by this Agreement. Notwithstanding any other provision of this Agreement, the arbitrator shall award costs to the party that substantially prevails in any arbitration proceeding, including recovery of that party's reasonable

attorney's fees, the arbitrator's fees, and all costs of litigation incurred by the prevailing party in connection with the arbitration. Nothing in this section shall restrict a party's right to seek injunction or other equitable relief in any court of competent jurisdiction prior to initiating arbitration.

15. Nondisclosure. Any information, trade secrets, know-how or proprietary information, in any form, that the parties hereto exchange shall be treated as confidential, shall be used only for the purpose of performing their respective obligations hereunder, and shall not be reproduced in whole or in part or disclosed to any other person for any other purposes. All such information shall be returned promptly upon demand of the discloser. The parties shall ensure that no information is shared with any third party except where necessary to perform the disclosing party's obligations under this Agreement and, in such cases, the disclosing party shall obtain a similar undertaking to preserve confidentiality from the third party.

The parties further agree to be responsible for the actions of their employees and any other person provided access to their offices who may have contact with or access to information subject to this Agreement, and to monitor those persons such that said information is continuously protected.

It is expressly agreed that a remedy at law for breach of the obligations set forth in this section concerning Nondisclosure is inadequate and that each party shall, in addition to any other remedies permitted by the Agreement, be entitled to injunctive relief to prevent the breach or threatened breach thereof.

All rights and obligations contained in this Agreement concerning the nondisclosure and protection of proprietary and confidential information shall survive the termination of this Agreement.

16. Notices. Except as otherwise specifically set forth in this Agreement, all notices, demands, requests or other communications that are required to be given by any party pursuant to this Agreement shall be in writing and shall be personally delivered, mailed by first-class registered or certified mail (return receipt requested and postage prepaid), or sent by courier, addressed as follows:

If to TokenEx:

Attention: Alex Pezold  
Address: P.O. Box 521068  
Tulsa, OK 74152-1068  
Phone: 877.316.4544  
Fax: 405.703.5277

If to Client:

Attention:  
Address:  
Phone:  
Fax:

17. Security Assessments and Audits. Upon reasonable request and no more than once every twelve (12) months, Client, one of Client's designated clients, or a representative of either of these parties, may

notify TokenEx in writing of Client's intent to conduct either an assessment or an audit of TokenEx relevant to the services being provided to Client by TokenEx, in order to assess the performance of TokenEx's obligations under this Agreement. For purposes of this paragraph, an "assessment" includes responding to written questions and providing limited documentation in respect of the services being provided Client by TokenEx; and, an "audit" includes both an assessment and a site visit including access to TokenEx's facilities, systems, personnel, and records pertaining to services provided to Client or Client's client. Client shall provide written notice to TokenEx of Client's intent to exercise these assessment or audit rights no less than thirty (30) days prior to initiation of any such assessment or audit. The notification shall contain the anticipated start date of the assessment or audit, questions to be answered, documents to be produced or reviewed, areas to be reviewed, and, in the event of an audit, the anticipated on-site arrival date of the auditors. All audits shall be conducted in a reasonable manner during normal business hours and shall not interfere with TokenEx's business. TokenEx will bear internal costs incident to any such audit (salary of affected employees, etc.) of TokenEx, but only to the extent of One Thousand dollars (\$1,000.00) per audit. Any internal expenses due to salary, etc., in excess of One Thousand dollars (\$1,000.00) per audit, shall be billed to Client at TokenEx's normal hourly rates. Each party shall communicate in good faith to agree to terms for an audit visit and adhere to these terms and admit properly identified and authorized employees or representatives of Client or Client's client onto TokenEx's premises. Such access shall be limited to TokenEx's facilities, systems, personnel and data that relate to the services provided to Client or a designated representative of Client. Copies of records that contain commingled documents or data of TokenEx that is not subject to audit or of TokenEx's other clients shall be provided to the auditing party upon reasonable request after documents and data not subject to audit has been removed

18. Business Continuity and Disaster Recovery Plans. Upon request, TokenEx shall promptly provide to Client an outline of TokenEx's business continuity and disaster recovery plan, testing and exercise documentation, and/or recovery strategies of TokenEx's contractors or subcontractors.

19. Security Controls. TokenEx has implemented and maintains (a) administrative, technical, and physical safeguards and security controls, (b) data retention, and incident response policies and procedures, and (c) an architecture designed for high-availability that is tailored to and appropriate for the nature and complexity of the Services, and otherwise designed to (i) ensure the security and confidentiality of the Services, personal information, and client data, (ii) protect against any anticipated threats or hazards to the security or integrity of the Services, personal information, and the client data, and (iii) protect against unauthorized access to or use of the Services, personal information, or the client data that could result in substantial harm or inconvenience to Client, Client's affiliates, or Client's clients or employees.

Updating of Security Controls. TokenEx shall evaluate and adjust TokenEx's security controls to (a) address any reasonable changes or additions to the services, TokenEx's operations, or the relationship between the parties, (b) address any risks or vulnerabilities reported to or discovered by TokenEx, (c) meet evolving industry standards and best practices, (d) comply with and respond to any changes in privacy laws or other applicable laws, and (e) address any other circumstances that TokenEx believes may have a material impact on the services, or could adversely affect Client, Client's affiliates or Client's employees or clients. TokenEx shall promptly correct any deficiencies or vulnerabilities identified as part of any monitoring, testing, or auditing. Without limiting the foregoing, TokenEx shall develop and implement an action plan for prompt corrective action to eliminate the identified risk, make the action plan available to Client, and provide all information reasonably requested by Client and Client's regulators in connection with the implementation thereof.

TokenEx shall notify Client in writing or via email immediately and in accordance with TokenEx's Incident response policy in the event of any known or suspected breach of confidentiality or security affecting Client, Client's affiliates, employees, relevant contractors or clients, including any known or suspected unauthorized access to or misuse, loss, alteration or destruction of personal information or other client data. The initial communication shall describe the nature and impact of the security incident, the actions already taken, and an assessment of the immediate risk. TokenEx shall cooperate in taking all reasonable actions necessary to investigate, respond to, and limit the adverse effects of the security incident on a basis no less favorable than offered to any other affected client, and shall participate in Client's internal incident response plan where applicable. TokenEx shall coordinate with Client regarding any notification to regulators, law enforcement, affected individuals, and the press, and shall not notify or otherwise contact any employees or clients of Client without Client's prior written approval.

20. PCI DSS Compliance. TokenEx has established security procedures and shall make reasonable efforts consistent with industry standards to protect cardholder data, meet all applicable audit requirements and comply with PCI DSS (hereinafter "Payment Card Industry Data Security Standards") and such other applicable rules, regulations, codes of practice, guidance and industry standards related to the handling and processing of credit card data in force from time to time during the term of this Agreement ("Payment Card Issuer Requirements"), as put forth by the PCI Security Standards Council.

TokenEx is responsible for the security of cardholder data TokenEx possesses or otherwise stores, processes, or transmits on Client's behalf, or to the extent TokenEx could impact the security of Client's cardholder data environment.

TokenEx agrees to comply with all applicable PCI DSS requirements to the extent that TokenEx handles, has access to, or otherwise stores, processes or transmits Client's cardholder data, or manages Client's cardholder data environment.

TokenEx acknowledges that TokenEx is solely responsible for compliance with all applicable PCI DSS requirements for TokenEx's tokenization products and services, including but not limited to, TokenEx's tokenization application programming interface (API), web site/pages, and vaulting services. Client agrees to monitor TokenEx's PCI DSS compliance at least annually.

TokenEx agrees that on request, TokenEx shall provide Client proof of the current status of TokenEx's PCI DSS compliance. If TokenEx or any of TokenEx's subcontractors are no longer in compliance with the Payment Card Issuer Requirements, TokenEx shall (a) notify Client of the same within twenty-four (24) hours of discovery by TokenEx, (b) implement compensating controls to mitigate risk for the non-compliance within seventy-two (72) hours of discovery of loss of compliance, and (c) develop and communicate a remediation plan and timeline for becoming compliant. If TokenEx fails to uphold the foregoing obligations Client shall have the right to terminate this Agreement or any part of the Services, and Client shall only be obligated to pay for any Products and/or Services satisfactorily delivered.

TokenEx agrees to comply with all applicable laws that require notification of individuals or parties in the event of unauthorized disclosure of cardholder data.

Pursuant to the provisions of this Agreement, in the event of a breach of any of TokenEx's security obligations relating to PCI or other event requiring notification under applicable law, TokenEx agrees to assume responsibility for informing all such individuals in accordance with applicable laws, and, subject to the indemnity and limitations on liability provisions contained herein.

21. Cooperation with Regulators. TokenEx shall provide reasonable cooperation to Client by providing service-specific information requested by Client's regulators or any of Client's clients concerning the relationship between the parties, and by making any modifications to the services and/or this Agreement required by such regulators. In the event that TokenEx determines that such modifications are impracticable or uneconomical, TokenEx shall have the right to terminate this Agreement.

22. Non-Competition. TokenEx agrees that during the term of this Agreement and for a period of one (1) year following the termination this Agreement, TokenEx shall not, directly or indirectly, solicit, recruit, employ or otherwise engage or attempt to engage as an employee, independent contractor or advisor any person who was an employee or independent contractor of Client during the term of this Agreement, or in any manner induce or attempt to induce any person who was an employee or independent contractor of Client during the term of this Agreement to terminate his or her relationship with Client.

TokenEx further covenants and agrees that during the term of this Agreement and for a period of one (1) year following termination of this Agreement, TokenEx shall not, directly or indirectly, solicit or attempt to solicit any of Client's customers or clients or engage in activity intended to redirect Client's business, to the extent that Client's business is the providing of electronic document management, workflow solutions, or finance processing services offered by Client during the term of this Agreement.

23. Force Majeure. Either party to this Agreement shall be released from liability hereunder for failure to perform any of its obligations hereunder where such failure to perform occurs by reason of any act of God, sabotage, war, strikes, lockouts, terrorism, military operations, national emergency, civil commotion, or the order, requisition, request or recommendation of any governmental agency or acting governmental authority, or by either party's compliance therewith, or governmental regulation or priority, or any other cause beyond either party's reasonable control whether similar or dissimilar to such causes. **In the event of any such disaster, TokenEx's release of liability hereunder is subject to TokenEx's reasonable execution of its Disaster Recovery and Business Continuity Plans, provided that any such exercise shall not itself have been rendered impracticable by any such event or its consequences.** TokenEx shall be obligated to perform and Client shall be obligated to pay for only such services actually performed during any of the above-mentioned conditions. If either party is not able to perform its material obligations under this Agreement within forty-five (45) days after the aforementioned conditions have been resolved or removed, then the other party may immediately terminate this Agreement. Such termination, however, shall not affect the rights or obligations of either party that have arisen or accrued prior to such termination.

#### 24. GENERAL PROVISIONS

Assignment. Neither party may assign or otherwise transfer this Agreement, or any of either party's rights or obligations hereunder, without the prior written consent of the other party, which consent shall not be unreasonably withheld.

Severability. In the event that any provision of this Agreement is invalid or unenforceable, such invalid or unenforceable provision shall not invalidate or affect the other provisions of this Agreement. The other provisions of this Agreement shall remain in effect and be construed as if the invalid or unenforceable provision were not a part hereof, provided that if the invalidation or unenforceability of such provision shall, in the opinion of either party, have a material effect on such party's rights or obligations under this Agreement, then the Agreement may be terminated by such party upon thirty (30) days' written notice by such party to the other party.



Entire Agreement. This Agreement, together with all documents incorporated by reference herein, constitutes the entire and sole agreement between the parties with respect to the subject matter hereof and supersedes any prior agreements, negotiations, understandings, or other matters, whether oral or written, with respect to the subject matter hereof. This Agreement and the terms of the parties' agreement cannot be modified, changed or amended except for in writing signed by a duly authorized representative of each of the party.

Headings. The headings in this Agreement are for convenience of reference only and shall not be considered in the interpretation of this Agreement.

Counterparts. This Agreement may be signed by facsimile and in one or more counterparts and, when signed by both parties, shall constitute a single binding agreement.

**[COMPANY]**

By \_\_\_\_\_  
Name \_\_\_\_\_  
Title \_\_\_\_\_  
Date \_\_\_\_\_

**TOKENEX**

By \_\_\_\_\_  
Name \_\_\_\_\_  
Title \_\_\_\_\_  
Date \_\_\_\_\_