Master Services and Data Sharing Agreement

Parties:

- **Bitlocus Exchange Ltd** – a company incorporated in Canada, incorporation number BC1520242, having its registered office at #319, 2300-2850 Shaughnessy St, Port Coquitlam BC V3C 6K5, Canada (hereinafter **"Party A"**).
- **Bitlocus Custody, Corp** – a company incorporated in the Republic of Panama, electronic folio no. 155785908 (hereinafter **"Party B"**).
- **"Client" or "Customer"** – any individual or entity that accesses or uses the services provided by Bitlocus Exchange Ltd or Bitlocus Custody, Corp, and agrees to this Agreement through electronic acceptance on the website or platform. (hereinafter **"Party C"**).

Party A, Party B, and Party C are each individually referred to as a "Party" and collectively as the "Parties."

RECITALS:

WHEREAS, Party A and Party B are engaged in financial services related to digital assets, which require implementing robust compliance procedures including Know-Your-Customer ("KYC") and Know-Your-Business ("KYB") verifications for clients;

WHEREAS, Party C wishes to obtain certain digital asset purchase, sale, transfer, custody, and related services from Party A and/or Party B, and acknowledges that such services are subject to strict legal and regulatory compliance requirements;

WHEREAS, Party A and Party B (and any future Party C joining this Agreement) desire to share with each other certain KYC and KYB information and documentation of their clients for the purposes of regulatory compliance, client onboarding, and other operational needs related to their financial services (the **"Permitted Purpose"**);

WHEREAS, the Parties recognize their obligations under their respective applicable local laws and regulations, including data protection and privacy laws, to protect Personal Data and to ensure that any cross-border transfer of such data is conducted lawfully and securely; and

WHEREAS, the Parties desire to formalize in this Agreement the terms and conditions of the services to be provided to Party C, as well as their respective rights and obligations regarding the sharing of KYC/KYB data, including provisions for data protection, confidentiality, consent mechanisms, and compliance with local laws.

NOW, THEREFORE, in consideration of the mutual covenants and promises herein, and for other good and valuable consideration, the sufficiency of which is acknowledged, the Parties hereby agree as follows:

1. Definitions

For the purposes of this Agreement, the following terms shall have the meanings set forth below. Other capitalized terms used in this Agreement shall be defined in context or shall bear the meaning ascribed to them by applicable law:

- **"KYC Data"** means personal identification information and documentation relating to individual clients, collected under Know-Your-Customer procedures. This includes, without limitation, full name, date of birth, government-issued identification documents (e.g. passport or driver's license), residential address, source of funds, and any due diligence notes or verification outcomes pertaining to the individual client.

- **"KYB Data"** means information and documentation relating to corporate or business clients collected under Know-Your-Business due diligence procedures, including business registration details, certificates of incorporation, shareholder or ownership information (including identification information of ultimate beneficial owners and directors), business addresses, and any related due diligence findings.

- **"Customer Due Diligence Information"** (or **"CDD Information"**) collectively refers to all information and documents obtained through KYC and KYB processes, including both KYC Data and KYB Data. This may include Personal Data of individuals (such as clients or beneficial owners) and business information of corporate clients.

- **"Permitted Purpose"** means the use of Customer Due Diligence Information by a receiving Party strictly for compliance with applicable laws and regulations (including but not limited to AML/CFT laws), for onboarding customers, ongoing monitoring, risk management, and other legitimate operational needs directly related to the customer's relationship with the Parties. The Permitted Purpose expressly excludes any use of the information for unsolicited marketing or for purposes unrelated to regulatory compliance or the customer's service needs.

- **"Applicable Laws"** means, with respect to each Party, all laws, statutes, regulations, rules, regulatory guidance, and government or court orders applicable to that Party's business or the subject matter of this Agreement. This includes, without limitation:

- For Party A (Bitlocus Exchange Ltd): Canadian federal and provincial laws and regulations relating to AML, KYC, and data protection, such as the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its regulations, guidance issued by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and applicable privacy legislation like the Personal Information Protection and Electronic Documents Act (PIPEDA) and/or any applicable provincial privacy laws.
- For Party B (Bitlocus Custody, Corp): Panamanian laws and regulations relating to AML, KYC, and data protection, including Law 23 of 2015 (Panama's primary AML law setting forth KYC obligations for financial institutions) and related regulations, Law 81 of 2019 (the Personal Data Protection Law of Panama) and its Executive Decree 285 of 2021, and any sector-specific rules (e.g. banking regulations) addressing data protection.

- For Party C: The laws and regulations of the jurisdiction in which Party C is incorporated or operates, concerning AML/KYC requirements and data protection/privacy, as well as any other laws to which Party C is subject in relation to the activities under this Agreement.

- **"Personal Data"** means any information relating to an identified or identifiable individual (natural person). For Party A, this term corresponds to "personal information" as defined under PIPEDA. For Party B, this corresponds to the definition of personal data under Panamanian Law 81 (i.e. information that identifies or makes an individual identifiable). KYC Data (and the portions of KYB Data that concern individuals, such as information on beneficial owners or directors) are considered Personal Data.

- **"Confidential Information"** means all information disclosed by one Party (the "Disclosing Party") to another Party (the "Receiving Party") under or in connection with this Agreement, whether in oral, written, electronic, or other form, that is identified as confidential or that reasonably should be understood to be confidential given the nature of the information and the context of disclosure. **Confidential Information** includes, without limitation: (i) all Customer Due Diligence Information (KYC/KYB Data) shared under this Agreement; (ii) any personal data or sensitive business information about the Parties' customers or clients, as well as non-public information about a Party's business plans, strategies, or processes; and (iii) the terms and existence of this Agreement, and any other non-public information regarding a Party's business operations, compliance strategies, or technology. **Confidential Information** does not include information that the Receiving Party can demonstrate: (a) is or becomes generally available to the public through no breach of this Agreement by the Receiving Party; (b) was already known to or in the possession of the Receiving Party on a non-confidential basis prior to disclosure by the Disclosing Party; (c) is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information; or (d) is rightfully obtained by the Receiving Party from a third party who has the lawful right to disclose such information without confidentiality obligations.

(Additional terms used in this Agreement may be defined contextually within later sections. Any references to statutes or regulations include such instruments as amended or replaced from time to time.)

2. Parties and Roles

2.1 **Independent Parties:** The Parties are entering into this Agreement as independent contracting entities. Nothing in this Agreement shall be construed to create a partnership, joint venture, agency, or franchise relationship among any of the Parties. Each Party is and will remain solely responsible for its own obligations, operations, and compliance with Applicable Laws, as well as for the actions of its own officers, employees, and agents.

2.2 **Designated Contacts:** Each Party shall designate one or more authorized contact persons (for example, appropriate compliance officers or data protection officers) who will be responsible for requesting and receiving KYC/KYB Data under this Agreement and for handling day-to-day communications between the Parties related to the sharing of such data. Within five (5) business

days of the Acceptance Date (or, for Party C, upon joining this Agreement), the Parties shall exchange in writing the names and contact details of their designated contact persons. Each Party may update its designated contacts as necessary by providing written notice to the other Parties.

(The Third Party (Party C) is included in this tri-party Agreement as a direct participant rather than a placeholder. If, in the future, an additional party is to be added to the data-sharing arrangement, such addition shall be accomplished only by a written amendment or joinder agreement signed by all existing Parties, wherein the new party agrees to be bound by all terms of this Agreement as a "Party." Unless and until any such additional party is added, all references to Party C or Third Party in this Agreement refer to the current Party C signatory above.)

3. Services

Party A and/or Party B (as applicable) shall provide Party C with services related to the purchase, sale, transfer, and custody of digital assets, including but not limited to Bitcoin and other supported cryptocurrencies. These services may be extended by the Bitlocus entities to include related consulting, compliance support, provision of white-labeled platforms, and other ancillary activities as agreed by the Parties in writing from time to time.

4. Execution of Transactions

Party C shall initiate cryptocurrency transaction requests via authorized communication channels specified by Party A or Party B. Upon receipt of a transaction request from Party C, the receiving Party (Party A or Party B) will provide a real-time quotation for the requested transaction. Once Party C accepts the quoted price or exchange rate, the relevant Party A or Party B shall execute the transaction and settle the corresponding fiat currency or digital assets to the designated wallet or account provided by Party C. The Parties acknowledge that the exchange rate for any digital asset transaction is determined at the time Party C accepts the quotation; such rates may vary depending on market conditions and other factors until acceptance, and the final executed rate will be the rate approved by Party C at the moment of transaction confirmation.

5. Risk Acknowledgment

By entering into this Agreement and using the services provided by Party A or Party B, Party C acknowledges and agrees that trading or investing in digital assets is inherently high-risk. Digital assets are not legal tender in most jurisdictions and are subject to unpredictable and volatile price fluctuations. **Party C understands that engaging in digital asset transactions may result in partial or total loss of assets.** Party C further acknowledges that Party A and Party B are not members of any investor protection scheme, and that Party C assumes all risks associated with using the services. Party A and Party B shall not be liable for any losses incurred by Party C as a result of market fluctuations or other risks inherent in digital asset transactions.

6. Fees and Payment

Party C agrees to pay the applicable fees charged by Party A and/or Party B for the services rendered under this Agreement. Such fees shall be communicated in writing (for

example, in a fee schedule, order form, or transaction quotation) and shall be deducted at the time of each transaction from the transaction funds or proceeds. No invoices shall be issued, and Party A and Party B shall not extend credit or assume any financial risk in connection with any transaction.

7. Transfers of Funds

Party A and Party B each reserve the right to reject or require additional verification for any incoming or outgoing funds transfer related to services under this Agreement. In particular, an incoming fiat wire transfer or digital asset transfer to any Party's platform or account may be held unprocessed until the sending Party has received sufficient confirmation or documentation (for example, a bank wire receipt) and any required "Travel Rule" information regarding the originator and beneficiary as mandated by Applicable Laws. Each Party will not fulfill a transaction or disburse exchanged funds until all required information—such as the ultimate destination account for fiat or digital assets and any necessary source-of-funds or beneficiary details—has been provided by Party C and verified to that Party's satisfaction.

If Party A or Party B cannot render the intended service or complete a transaction due to incomplete information or legal impediments, the Party may still charge any applicable transaction or processing fee for the attempt. Once a service is fulfilled and funds (fiat or digital assets) are delivered to Party C's designated account or wallet, the delivering Party bears no responsibility for those funds thereafter. Party C understands that after delivery confirmation, all risks of loss or theft of the assets pass to Party C.

8. Taxes

Each Party shall be solely responsible for determining the taxes (if any) that apply to transactions and services under this Agreement. Party C is solely responsible for evaluating and fulfilling any tax obligations arising from its use of the services, including any required withholding, collection, reporting, or remittance of taxes to relevant tax authorities. Party A and Party B make no representations regarding the tax consequences of any transaction and shall not be responsible for advising Party C on tax matters. Party C should seek professional tax advice if necessary to ensure compliance with all tax laws applicable to its activities.

9. Exchange Rate

Party A or Party B (as the case may be) will execute digital asset purchase or sale transactions for Party C based on the exchange rate quoted and approved by Party C at the time of the transaction. Party C acknowledges that digital asset exchange rates are subject to market volatility and may fluctuate rapidly. The exchange rate provided in a quotation is valid only at the time it is given, and the executed rate will be the one accepted by Party C when it confirms the transaction. The Parties agree that any exchange rate information provided prior to execution is for reference only and that the final binding rate is the one documented at the moment of transaction execution.

10. Promotions

Party A or Party B may, from time to time and in their sole discretion, offer promotional deals, discounts, or incentives related to their services. **Party C acknowledges that not all promotions or discounts will be applicable to Party C's situation.** The availability and eligibility requirements for any promotion or discount shall be determined by the offering Party. Party A and Party B reserve the right to initiate or terminate any promotional program or discount at any time without advance notice. Participation in any promotion is subject to any additional terms and conditions that may be provided by the offering Party.

11. Compliance and Data Sharing

11.1 Compliance with Local KYC/AML Laws: Each Party shall comply with all Applicable Laws in its home jurisdiction relating to customer identification, verification, due diligence, record-keeping, and the reporting of suspicious activities. Each Party represents that it holds any licenses or registrations that are legally required for its operations (for example, registration as a money services business or other financial institution, if applicable) and for carrying out the activities contemplated under this Agreement. For example, Party A shall adhere to Canadian AML regulations under the PCMLTFA and FINTRAC guidance, and Party B shall adhere to Panamanian KYC requirements under Law 23 of 2015 and related regulations. Each Party remains individually responsible for fulfilling its legal requirements to verify customer identity, identify beneficial owners, conduct ongoing monitoring, and report suspicious transactions to the appropriate authorities in its jurisdiction.

11.2 Sharing of KYC/KYB Data: Subject to the terms of this Agreement, each Party agrees to share relevant KYC Data and KYB Data with the other Party/Parties for the Permitted Purpose. Such sharing will occur on a reciprocal, as-needed basis. For instance, if a client of Party A seeks to use a service offered by Party B (or vice versa), then upon request, Party A shall provide Party B with the necessary KYC/KYB information about that client so that Party B can satisfy its own compliance obligations for onboarding or monitoring that client (and vice versa). The Parties shall share Customer Due Diligence Information in good faith and in a timely manner, using secure communication channels as agreed (see Section 12.3 on security measures).

11.3 Permitted Purpose – Use Limitations: The Receiving Party shall use any Customer Due Diligence Information obtained from another Party solely for the **Permitted Purpose** as defined in Section 1. Under no circumstances will a Receiving Party use shared KYC/KYB Data for any purpose outside the scope of compliance, onboarding, or operational needs directly related to servicing the relevant customer. In particular, the Receiving Party shall **not** use the information for marketing or solicitation of the customer, nor disclose it to any external third party (except as permitted by this Agreement or as required by law, and then only in accordance with Section 13 on Confidentiality). Each Party acknowledges that misuse of Personal Data beyond the stated purpose could violate privacy laws as well as the terms of this Agreement.

11.4 Accuracy and Currency of Data: Each Party will use reasonable efforts to ensure that the KYC/KYB Data it shares is accurate, up-to-date, and as complete as necessary for the stated purposes at the time of sharing. This obligation includes sharing the most current copies of identification documents or corporate information on file, and promptly notifying the other

Parties if it becomes aware that any data previously shared has become outdated or contains material inaccuracies. For example, if a customer's identification document on file has expired or a business client has changed its ownership structure, the Party that originally collected the data will update that information and, where relevant, inform the other Party/Parties relying on that data.

11.5 Ongoing Due Diligence & Monitoring: Each Party retains responsibility for conducting ongoing due diligence on the customers it directly services. The sharing of KYC/KYB data under this Agreement is intended to facilitate each Party's compliance, but does not absolve any Party from continuing to monitor transactions or update customer information as required by its own policies and Applicable Laws. If a Party (the "Notifying Party") detects suspicious activities or any change in a shared customer's risk profile that might be relevant to another Party's compliance efforts (for instance, if a customer common to both Party A and Party B is flagged for suspicious transactions or appears on a sanctions list), the Notifying Party shall—**to the extent permitted by law and without tipping off the customer**—inform the other relevant Party/Parties promptly so that appropriate measures can be taken in coordination.

11.6 Reliance on Collected Data: To the extent allowed by their local regulations, the Parties may rely on the KYC/KYB checks performed by another Party when onboarding or reviewing a customer, provided that: (a) the Party that originally collected the data (the "Originating Party") represents that it followed all required customer identification procedures under its local law (which are at least as stringent as the relying Party's own requirements); and (b) the Originating Party agrees to furnish copies of the underlying identification documents and due diligence records without undue delay upon request (see Section 12.4 below regarding data access requests). Each Party acknowledges that under international standards (e.g., Financial Action Task Force Recommendation 17), when one financial institution relies on another for customer due diligence, the ultimate responsibility for compliance remains with the relying institution, and necessary customer information should be obtained immediately with verification documents available upon request. Accordingly, each Party will remain fully accountable to its regulators for the KYC/KYB obligations on its customers even when it relies on data or checks performed by another Party, and nothing in this Agreement transfers or delegates legal responsibility for KYC failures to any other Party.

11.7 Obtaining Consent and Legal Basis: Each Party shall ensure that it has a proper legal basis to collect and to share the Customer Due Diligence Information with the other Parties. In particular, where required by Applicable Laws, each Party will obtain the customer's consent to share their Personal Data with affiliates or third parties for compliance and service purposes. For example, Panama's data protection law generally requires prior, informed, and unequivocal consent from the data subject for transferring Personal Data, unless an exception applies. Each Party confirms that nothing in its applicable privacy or bank-secrecy laws prohibits it from sharing the KYC/KYB Data with the other Parties as contemplated herein, and that it has obtained any customer consents or provided any notices required to legitimize such data sharing. If a Party's law permits the sharing of customer data within the same corporate group without explicit consent (such as transfers within a financial group for the same original purpose), that Party will ensure that all conditions for such permitted sharing are met. Each Party shall maintain records evidencing that proper consent was obtained from the customer (or that a lawful exception applies) for audit purposes.

11.8 Local Law Constraints and Notifications: If at any time a Party becomes aware of any legal impediment to either sharing or receiving certain data (for instance, a change in law that restricts cross-border data transfers or imposes new conditions), that Party shall promptly notify the other Parties in writing. The Parties shall then cooperate in good faith to find a compliant solution, which may include obtaining additional customer consents, adopting enhanced safeguards, or—if no solution is available—limiting or ceasing the affected data transfers. No Party shall be required to share data in violation of its local laws. If a Party cannot provide certain information requested by another Party due to a legal restriction, it shall explain (to the extent permissible) the nature of the restriction and work with the requesting Party to provide alternative evidence or to arrange a lawful method of compliance.

11.9 Training and Awareness: Each Party shall ensure that its relevant personnel (including compliance officers and any employees involved in handling or requesting KYC/KYB Data from other Parties) are trained on and aware of the requirements of this Agreement. Such personnel should understand the confidential nature of the data, the limited purposes for which it may be used, and the procedures to follow to request or transmit data securely. Regular training or refresher sessions shall be provided, especially when there are updates in Applicable Laws or internal policies that affect how customer data is shared or protected.

11.10 Record-Keeping: Each Party shall keep records of all Customer Due Diligence Information it collects, as well as records of any data requests and transfers made under this Agreement, in accordance with its local record-retention requirements. At a minimum, and subject to any stricter requirements of Applicable Laws, each Party will retain copies of KYC/KYB data and related records for at least five (5) years from the end of the customer relationship or the date of the transaction or data exchange, whichever is later. (For example, Panama requires entities to keep KYC records for a minimum of 5 years for audit purposes, and other jurisdictions may require longer retention.) If local law requires a longer retention period (e.g., 7 years), or an extended retention due to an ongoing investigation, the Party will retain the records accordingly. Upon termination of this Agreement or upon a Party's departure, each remaining Party shall continue to preserve any shared records as required by law.

11.11 Audits and Assurance: To build mutual trust in the shared data, each Party agrees that any other Party may, upon reasonable notice and at most once annually, request to conduct (or have an independent auditor conduct) a review or audit of specific controls of the other Party that are relevant to the execution of this Agreement. Such audits might include reviewing procedures for collecting KYC data, how customer consent is obtained, or the security measures in place for data protection. The scope of any audit shall be mutually agreed in advance and shall be limited to verifying compliance with this Agreement and applicable data protection/AML obligations, without unduly intruding into unrelated aspects of the audited Party's business. Each Party shall reasonably cooperate with such audits or inquiries, and may require that auditors sign appropriate confidentiality agreements. Unless otherwise agreed, each Party will bear its own costs for any such audit. However, if a material breach of this Agreement is discovered through an audit, the breaching Party shall reimburse the reasonable audit expenses of the other Party/Parties.

11.12 Notification of Regulatory Changes or Inquiries: Each Party will promptly inform the others if it becomes subject to any regulatory inquiry, investigation, or enforcement action that is directly relevant to the KYC/KYB data-sharing activities under this Agreement. For example, if

a regulator in one Party's jurisdiction raises a concern about the legality of sharing customer data abroad, or if a data protection authority or financial regulator requests information about the sharing arrangement, the affected Party shall (to the extent legally permitted) notify the other Parties of the inquiry and the nature of the information sought. The Parties will then consult with each other on an appropriate response or adjustment to their practices, ensuring transparency and continued compliance.

11.13 Suspension of Services for Non-Compliance or Misuse: Each Party reserves the right to restrict, suspend, or terminate a customer's access to services or any data-sharing under this Agreement, without prior notice, if it determines that the customer or another Party has failed to provide required Customer Due Diligence Information, has violated Applicable Laws, or has used the services or site in a manner that is abusive or designed to circumvent controls. In particular, if Party C does not provide requested KYC/KYB information or if Party A or Party B identifies Party C's involvement in fraud, money laundering, terrorist financing, or any other illegal activity, Party A or Party B (as appropriate) may immediately suspend transactions or lock down Party C's accounts or assets pending further investigation. Party C **waives any and all claims** against Party A or Party B arising from any such suspension or termination of access implemented in good faith in accordance with this Agreement.

11.14 Updating Information: Party C (and each Party, as applicable) shall promptly update the other Parties if any previously provided Customer Due Diligence Information changes or becomes outdated. Additionally, each Party may require re-validation of identity when Party C or any customer updates certain profile information. For example, if Party C requests changes to its authorized representatives or account details, Party A or Party B may require Party C to provide a fresh government-issued ID or other verification documents for the new information as part of ongoing due diligence and fraud prevention measures.

11.15 Identity Verification Authorization: Party C acknowledges that Party A and Party B may be required by law to verify Party C's identity and undertake other background checks. Party C agrees to provide promptly, upon request, any personal or business information that Party A or Party B deems necessary to comply with their obligations (including but not limited to name, address, telephone number, email address, date of birth or incorporation, government identification numbers, financial account details, etc.). Party C **authorizes** Party A and Party B to make any inquiries they consider necessary to verify identity and to assess compliance risks, including querying information contained in public records or databases, verifying information associated with Party C's bank accounts or digital asset wallets, and obtaining reports from credit bureaus or other background-check services. Party C further authorizes all third parties (such as banks, credit agencies, and government authorities) to provide information in response to such inquiries. Each Party agrees that any identity verification information obtained about Party C shall be treated in accordance with the data protection and confidentiality provisions of this Agreement.

12. Data Protection and Security

12.1 Compliance with Data Protection Laws: Each Party shall handle all Personal Data received from the other Parties under this Agreement in accordance with all applicable data protection and privacy laws. For Party A, this includes compliance with PIPEDA (and any relevant provincial

privacy laws); for Party B, this includes compliance with Panama's Law 81 of 2019 and related regulations on personal data protection, as well as any data protection obligations under applicable AML laws. Party C shall likewise comply with the data protection laws of its jurisdiction in relation to any Personal Data it processes under this Agreement. Each Party is deemed to be a separate data controller (or equivalent term under local law) for any Personal Data it receives and processes under this Agreement, determining the purposes and means of processing such data for its own operations. No Party will process Personal Data received under this Agreement in a way that the Disclosing Party itself could not lawfully do. Each Party confirms that it has implemented, and will maintain, appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure, as required by Applicable Law. (For example, Panama's Law 81 mandates data controllers to establish secure data management and transfer procedures to protect data subjects' rights, and Canada's PIPEDA requires safeguards appropriate to the sensitivity of the information.)

12.2 Cross-Border Transfer Safeguards: The Parties acknowledge that sharing KYC/KYB Data under this Agreement will involve cross-border transfers of Personal Data (for instance, between Canada and Panama, and potentially to or from Party C's jurisdiction). The Parties shall ensure that such transfers are conducted in compliance with the requirements of their respective data protection laws governing international data transfers. By entering into this Agreement, the Parties are also putting in place a contractual framework designed to safeguard Personal Data in transit and in use, thereby meeting certain legal conditions for cross-border transfer. For example, Canada's PIPEDA permits transferring personal information to foreign third parties for processing or use, provided appropriate safeguards and contractual measures are in place to protect that data. Likewise, Panama's Law 81 allows cross-border transfers of Personal Data if specific conditions are met, such as obtaining the data subject's consent or ensuring the recipient affords an equivalent level of data protection, or by implementing contractual clauses with data protection mechanisms in line with Panamanian law. Each Party warrants that, to the extent required under its laws, it has satisfied one or more legal bases for international data transfer – such as obtaining customer consent for the transfer, transferring within the same corporate group under equivalent safeguards, and/or using standard contractual clauses or binding corporate rules as applicable. If at any point a data protection authority determines that additional measures are needed for compliance (for example, updated contract clauses or specific notices to individuals), the Parties agree to promptly work together in good faith to implement such measures.

12.3 Security Measures: Each Party shall apply industry-standard security measures to the storage and transmission of Customer Due Diligence Information shared under this Agreement. At a minimum, this includes: encryption of Personal Data during transmission between the Parties (for example, using encrypted email, secure file transfer protocols, or providing access via a shared secure portal); access controls to ensure that only personnel with a strict "need-to-know" (such as designated compliance or legal officers) can access the data; and logical security measures such as strong authentication procedures, firewalls, intrusion detection systems, and up-to-date malware protection. Each Party shall also maintain physical security for any hard-copy documents (e.g. storing files in locked cabinets within secure office facilities). Security protocols shall be reviewed and tested periodically, and any identified vulnerabilities shall be addressed promptly. If a Party engages any subcontractor or agent to assist in processing shared data (for example, a secure cloud service provider or data analytics contractor), that Party

remains responsible for protecting the data and must ensure the subcontractor is bound by equivalent data protection and confidentiality obligations. The Party engaging the subcontractor will remain liable for any actions or omissions of such subcontractor with respect to the shared data.

12.4 Data Access Requests: Upon reasonable request by one Party, another Party shall provide access to specific KYC/KYB documents or information in its possession that relate to a customer of the requesting Party, to the extent such access is needed for compliance purposes. For instance, if Party B needs to see a copy of a customer's identification document that Party A originally collected, Party A will furnish a clear copy of that document to Party B promptly. The Parties commit to respond to such requests without undue delay, recognizing that efficient access is crucial (for example, if regulators demand evidence of due diligence during an examination). As a guideline, the Parties will aim to fulfill requests within a few business days (and, if urgent and feasible, within 24–48 hours). If a Party cannot share the requested information (due to a legal restriction or because it does not have it), it should promptly inform the requesting Party and cooperate to find an alternative solution. All such inter-party requests and the transfers of information should be logged by both sides for audit trail purposes (noting the date of request, who requested, what information was provided, and for what purpose).

12.5 Data Quality and Updates: The Parties shall establish a process to keep shared KYC/KYB Data updated. If any Party receives new or updated information about a customer that is materially relevant (such as renewed identification documents, a change of address, a change in the ownership structure of a business client, or the discovery that previously provided documents were fraudulent or inaccurate), that Party should inform any other Party who has received or is relying on the earlier data, so that the other Party can update its records and remain compliant. Conversely, if a receiving Party itself, through its own interactions with the customer, obtains updated information (for example, Party B obtains a new address from a customer that was originally onboarded by Party A), Party B should consider informing Party A so that both Parties' records remain consistent, subject to any legal constraints. The Parties may also agree to conduct periodic checks (e.g. quarterly or semi-annual) where they compare notes to see if any shared customers have updated KYC records that should be exchanged.

12.6 Data Minimization: The Parties agree to limit KYC/KYB data sharing to what is necessary for the Permitted Purpose. Each request for data under this Agreement should be tailored to only the information that the requesting Party genuinely requires for compliance or onboarding of the specific client. For example, if Party A only needs to verify the identity and address of a client that Party B has already vetted, Party B need not send excessive data beyond what confirms identity and address (unless additional due diligence information is needed for risk assessment). The Parties will avoid wholesale or bulk transfers of entire databases of customer information, unless such a transfer is specifically justified by an operational need and permitted by law (e.g., in the context of a corporate acquisition or merger, which would be handled via a separate agreement or addendum). In cases of doubt, the Parties' compliance officers shall communicate to ensure that the principles of data minimization are respected.

12.7 Personal Data Subject Rights: Each Party is responsible for handling any requests or complaints from individuals (data subjects) whose Personal Data may be shared under this Agreement, in accordance with that Party's own obligations under Applicable Laws (such as an

individual's right to access their personal data, or to request correction or deletion, etc.). If a Party receives a data subject request that pertains to data originally provided by another Party, the receiving Party shall, if necessary, consult with the other Party to obtain the information needed to respond. For instance, if an individual asks Party A, "What information of mine have you shared with Party B?", Party A may need to confer with Party B to confirm what was shared. The Parties agree to provide reasonable assistance to each other in responding to data subject requests or regulatory inquiries related to Personal Data that was shared, so that each Party can fulfill its legal obligations. If an individual withdraws consent for the processing or sharing of their Personal Data (and consent was the legal basis for sharing), the Party that receives such withdrawal shall promptly inform the other Party/Parties, and all Parties will cease any further sharing or use of that individual's data under this Agreement unless another legal basis permits continuing the processing.

12.8 Data Breach Notification: Each Party shall maintain an incident response plan to handle any suspected or confirmed **Personal Data Breach** (meaning a security incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data) involving KYC/KYB Data shared under this Agreement. In the event a Party (the "Breached Party") discovers a data breach that compromises any Customer Due Diligence Information received from or shared by another Party, it shall notify the other Parties without undue delay—and in no event later than 72 hours of becoming aware of the breach, where feasible. The Breached Party's notification to the other Parties shall include, to the extent known at the time, sufficient details about the nature of the breach, the data affected, and any remedial actions taken or planned. The Breached Party will promptly take all necessary steps to contain and remediate the breach, such as isolating affected systems, patching vulnerabilities, and recovering data. The Parties will cooperate in good faith in addressing the breach's consequences – for example, coordinating any required notifications to regulators or affected individuals (noting that under certain laws, such as Panama's Law 81, breaches posing a risk must be reported to the data authority and affected subjects within 72 hours, and under Canadian law and other jurisdictions, breaches meeting certain harm thresholds must be reported to privacy commissioners and individuals). Each Party agrees that it will not disclose specifics of a breach to any unrelated third party (except to regulators or as required by law) without first consulting the other affected Party/Parties, to the extent such consultation is feasible.

12.9 Cross-Border Storage and Processing: The Parties acknowledge that once KYC/KYB Data is shared, it will be stored and processed in the jurisdiction of the receiving Party and possibly in other jurisdictions (for example, if a Party uses cloud storage or centralized databases located in another country). Each Party will be transparent (in its privacy notices to customers and in communications with the other Parties) about where and how it stores shared Personal Data. For instance, Party A will inform its customers that their personal information may be transferred to and stored in Panama (and/or any other relevant country, including Party C's jurisdiction) for compliance purposes, and that while abroad it may be subject to the laws of that foreign jurisdiction. Party B will likewise ensure that individuals are informed if their data may reside in Canada or any other country due to the data-sharing under this Agreement. Each Party agrees that, regardless of where it stores or processes the data, it will ensure protection consistent with the requirements of this Agreement and with the standards of its home jurisdiction's data protection laws.

12.10 Data Return or Deletion: Subject to the record-keeping requirements described in Section 11.10 and any overriding legal obligations, upon the termination of this Agreement or upon written request of a Disclosing Party, each Receiving Party shall promptly return or securely destroy any KYC/KYB Data it has received from the other Parties that is no longer necessary for the Permitted Purpose. **Destruction** shall include shredding of physical documents and permanent deletion of electronic files (with reasonable measures taken to prevent recovery). If a Party is required by law or by a government regulator to retain certain data (for example, to satisfy an audit requirement or an ongoing inquiry), it may retain a copy but must continue to protect that data under the terms of this Agreement and Applicable Laws, and shall destroy it once the legal retention period expires or the investigation concludes. At the Disclosing Party's request, the Receiving Party will provide written certification by an officer that all applicable Confidential Information or Personal Data has been returned or destroyed in accordance with this clause.

13. Confidentiality

13.1 Confidentiality Obligations: Each Party, as a Receiving Party of Confidential Information (including any Customer Due Diligence Information) from another Party, shall: (a) keep all such Confidential Information strictly confidential and not disclose it to any third party except as expressly permitted by this Agreement or with the Disclosing Party's prior written consent; and (b) use the Confidential Information only for the Permitted Purpose and in accordance with the terms of this Agreement. The Receiving Party shall handle the Disclosing Party's Confidential Information with the same degree of care that it uses to protect its own confidential and proprietary information of similar importance, and in no event less than a reasonable standard of care. This means implementing appropriate administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of the Confidential Information.

13.2 Permitted Disclosures: Notwithstanding Section 13.1, a Receiving Party may disclose Confidential Information of a Disclosing Party under the following circumstances and to the following persons, but only to the extent necessary for the Permitted Purpose or as required by law: **(i)** to its own directors, officers, employees, or contract staff who *need to know* the information for compliance or operational purposes related to this Agreement, provided that such persons are bound by confidentiality obligations at least as protective as those in this Agreement; **(ii)** to its affiliates or service providers (for example, secure cloud storage providers or data management consultants) who need to process the information for the Party's compliance or data management purposes, provided that the Party has ensured those recipients are under contractual or professional duties of confidentiality and data protection that are no less stringent than those herein; or **(iii)** to regulators, auditors, examiners, or law enforcement authorities, but only to the extent that such disclosure is mandated by applicable law or regulation (for example, in response to a lawful subpoena, regulatory examination request, or court order). In the event a Receiving Party is required by law or regulatory directive to disclose Confidential Information, it shall, if legally permissible and practicable, give prompt notice to the Disclosing Party so that the Disclosing Party may seek an appropriate protective order or other remedy to prevent or limit the disclosure. Even if Confidential Information must be disclosed to authorities, the Parties will seek to ensure that it remains protected – for instance, by requesting confidential treatment of sensitive information in any regulatory or court filings.

13.3 Confidentiality of Customer Data: The Parties specifically acknowledge that the Customer Due Diligence Information shared under this Agreement contains highly sensitive personal and business data about customers. Each Party warrants that it has in place internal policies consistent with this Agreement that prohibit unauthorized sharing or misuse of customer information. (For example, financial institutions often have legal obligations to maintain the confidentiality of customer information, such as under Canadian banking privacy requirements or Panama's banking secrecy provisions.) By adhering to those obligations and this Agreement, the Parties agree, among other things, not to disclose a customer's personal or financial details to any third party except as allowed by this Agreement. This clause does not prevent a Party from using the information internally for compliance purposes, but any internal use must still respect principles of privacy and confidentiality (e.g., only personnel with relevant duties should access it).

13.4 No Publicity: No Party shall use the name, logo, or trademarks of any other Party in any public announcement, marketing material, or publicity related to this Agreement, nor will any Party disclose the existence or terms of this Agreement to any third party (except its professional advisors or as required by law), without the prior written consent of the other Parties. An exception to this is that if disclosure of this Agreement's existence or certain terms is required by law or regulation (for instance, a disclosure required in financial statements or regulatory filings), the disclosing Party shall, if feasible, notify the other Parties in advance of such disclosure. The Parties prefer to keep the existence and specifics of this data-sharing arrangement confidential, to avoid drawing undue attention or exposing details that could compromise security or competitive advantage.

13.5 Duration of Obligations: The confidentiality obligations set forth in this Section 13 commence on the Acceptance Date of this Agreement (and, for any Third Party added later, upon their joinder to the Agreement) and shall continue for the term of this Agreement and for a period of at least five (5) years after its termination or expiration. However, with respect to any Confidential Information that constitutes Personal Data or trade secrets, the obligation to protect such information shall survive indefinitely (or for the maximum period permitted by applicable law), until such information falls into one of the exceptions in the definition of Confidential Information (for example, becomes public through no breach of this Agreement). The termination of this Agreement shall not relieve any Party from its duty to protect Confidential Information received prior to termination.

13.6 Return/Destruction of Confidential Information: Upon termination of this Agreement, or upon written request of a Disclosing Party at any time, each Receiving Party shall promptly return to the Disclosing Party or destroy (as elected by the Disclosing Party) all Confidential Information of the Disclosing Party in the Receiving Party's possession or control that is in tangible form, and delete or render unrecoverable all electronically stored Confidential Information, **except** for such copies as the Receiving Party is required to retain under Section 12.10 (Data Return or Deletion) or applicable law for compliance purposes. Any retained information shall remain subject to the confidentiality and data protection provisions of this Agreement. At the Disclosing Party's request, an officer of the Receiving Party shall certify in writing that such return or destruction has been completed.

13.7 Unauthorized Disclosure Notification: If any Confidential Information of a Disclosing Party is, or is suspected to have been, accessed or disclosed by a Receiving Party (or its personnel) in an unauthorized manner or to an unauthorized person, the Receiving Party shall immediately notify the Disclosing Party and take all reasonably necessary steps to mitigate the effects of such disclosure and prevent any further unauthorized use or disclosure. This obligation is in addition to, and does not limit, the requirements of Section 12.8 (Data Breach Notification) with respect to Personal Data breaches. The Receiving Party shall cooperate fully with the Disclosing Party in investigating the incident, attempting to recover the information, and mitigating any damage. The Parties acknowledge that an unauthorized disclosure of personal or other highly sensitive Confidential Information may cause irreparable harm to the Disclosing Party or to the individuals whose data is disclosed; therefore, the Disclosing Party shall be entitled to seek immediate equitable relief (such as temporary or permanent injunctions) to prevent or remedy any such unauthorized disclosure, in addition to any other remedies available at law or in equity.

13.8 No Warranty on Information: Unless expressly stated elsewhere in this Agreement, all Confidential Information, including any KYC/KYB Data shared, is provided "as is." While each Disclosing Party shall strive for accuracy and completeness in the information it shares (per Section 11.4), no Disclosing Party makes any express or implied warranty or guarantee as to the accuracy, reliability, or completeness of its Confidential Information. The Receiving Party is solely responsible for its use of the information and should independently verify any critical elements (for example, each Party should perform its own sanctions screening, even if another Party has provided some screening results). Except in the case of fraud or willful misconduct by the Disclosing Party in providing data, each Party agrees that the Disclosing Party shall not be liable for errors or omissions in the Confidential Information it shares. *(This provision does not excuse any Party from liability for breach of confidentiality or data protection obligations; it pertains only to the quality or accuracy of information shared.)*

14. Representations and Warranties

Each Party represents and warrants to the others, as of the Acceptance Date (and with respect to Party C, as of the date it joins this Agreement), that:

(a) Organization and Good Standing: It is a legal entity duly organized, validly existing, and in good standing under the laws of its jurisdiction of incorporation or formation.

(b) Authority and Enforceability: It has the full right, power, and authority to enter into and to perform its obligations under this Agreement. The person(s) accept this Agreement on its behalf are duly authorized to do so, thereby binding the Party to the terms of this Agreement. This Agreement, once executed, constitutes a valid and binding obligation of that Party, enforceable against it in accordance with its terms.

(c) No Conflicts: Neither the execution and delivery of this Agreement, nor the performance of this Agreement or the consummation of the transactions contemplated herein, will conflict with or result in a breach of any other agreement, contract, or instrument to which the Party is bound, nor will it violate any law, regulation, or court order applicable to that Party.

(d) Sanctions and Eligibility: Neither the Party, nor any person owning or controlling the Party, nor any person acting on the Party's behalf (such as an officer or agent) is: (i) listed on any

government-issued sanctions list (including, without limitation, the U.S. Office of Foreign Assets Control's list of Specially Designated Nationals and Blocked Persons (SDN List)); (ii) a foreign shell bank or a shell company prohibited by Applicable Laws; or (iii) located in, organized under the laws of, or ordinarily resident in any country or territory that is subject to comprehensive economic sanctions or identified by the Financial Action Task Force (FATF) as a high-risk or non-cooperative jurisdiction, such that providing services or sharing data with that Party would violate Applicable Laws. Each Party further warrants that it shall notify the other Parties promptly if it, or any related person described above, becomes subject to any sanctions or listed in any sanctions program during the term of this Agreement.

(e) Licenses and Compliance: It holds and will maintain in force all governmental or regulatory licenses, permits, authorizations, or registrations necessary for the conduct of its business as presently conducted, and for the performance of its obligations under this Agreement. Each Party represents that it is in compliance with all Applicable Laws relevant to this Agreement, including those relating to anti-money laundering, counter-terrorist financing, anti-bribery, sanctions, and data protection, and that it will perform this Agreement in compliance with all such laws.

The representations and warranties in this Section 14 are deemed to be continuous in nature. Each Party shall be deemed to repeat each of the above representations and warranties at all times until the termination of this Agreement. If at any time a Party becomes aware that any of the above representations has ceased to be true with respect to itself, it shall promptly notify the other Parties in writing.

15. Disclaimer of Warranties (General and Suitability)

No Advice or Reliance: The Parties acknowledge that any content, information, or communications provided by Party A or Party B (whether via their websites, platforms, or otherwise) to Party C are for general information purposes only. Such content may include market data, analytics, news, or other information. **Party C should not regard any information provided by Party A or Party B as legal, tax, investment, financial, or other professional advice on which Party C can solely rely.** Party C is responsible for obtaining its own professional advice (legal, financial, or otherwise) tailored to Party C's situation before taking or refraining from any action in connection with the services or information provided under this Agreement. Although Party A and Party B may make reasonable efforts to ensure that information directly provided to Party C is current and accurate, neither Party A nor Party B makes any representation, warranty, or guarantee, express or implied, that any content or information provided to Party C is accurate, complete, up-to-date, or suitable for Party C's needs. Any decisions Party C makes in using the services or acting on information are at Party C's own risk.

Use at Own Risk: Party C's use of Party A's and Party B's services and any related platform or site is at Party C's own risk. The services are provided on an "as is" and "as available" basis, except as otherwise expressly set forth in this Agreement. To the maximum extent permitted by law, neither Party A nor Party B, nor any of their respective parent companies, subsidiaries, affiliates, nor any of their respective directors, officers, employees, agents, service providers, contractors, licensors, licensees, suppliers, or successors, makes any specific warranty of any kind, express or implied, regarding the services provided under this Agreement or any related

information, including any implied warranties of merchantability, fitness for a particular purpose, title, or non-infringement. Each of Party A and Party B, and their respective affiliates and personnel, expressly disclaims any responsibility or liability for Party C's use of the services, except as expressly provided in this Agreement.

No Recommendations or Investment Advice: Party A and Party B do not guarantee any outcomes or profitability in connection with Party C's use of the services. Neither Party A nor Party B is providing any investment, tax, or legal advice or making any recommendations to Party C in connection with any digital asset transactions or other services. Any decisions that Party C makes to buy, sell, exchange, or hold digital assets are solely Party C's own decisions, based on Party C's personal assessment of its financial situation and risk tolerance. Party C is solely responsible for evaluating the merits and risks associated with using the services and trading or holding digital assets. **Party C acknowledges that it has determined, on its own or in consultation with its advisors, that using the services of Party A and Party B and engaging in digital asset transactions is suitable for Party C's business or investment objectives and risk profile.**

16. Securities Law Compliance

None of the information provided by Party A or Party B (whether on their websites, through other communications, or via the services) constitutes a recommendation, solicitation, or offer for Party C or any other person to buy or sell any securities, futures, options, or other financial instruments, nor does it constitute the provision of any investment, tax, or legal advice or service, except as may be explicitly agreed in writing as part of a specific service.

Party A, Party B, and their affiliates are **not** registered as securities brokers or dealers, investment advisers, or any other form of investment or financial institution in any jurisdiction, unless expressly stated otherwise. In particular, Party A and Party B are not registered as investment dealers, advisors, or fund managers under Canadian securities laws, nor are they registered as an investment company under the U.S. Investment Company Act of 1940. Party A and Party B do not currently rely on any exemption from such registrations in providing the services under this Agreement.

Party C acknowledges that certain digital assets or tokens that Party A or Party B may facilitate transactions in could potentially be considered "securities" in one or more jurisdictions (for example, under Canadian securities laws). Any such transactions involving Party C will only be carried out in compliance with Applicable Laws and any necessary exemptions. For instance, if a particular digital asset is deemed a security in Canada, Party C represents that it qualifies to purchase or sell such asset under a private placement or other exemption from the prospectus requirements, and Party C will only engage in transactions through appropriately registered or exempt intermediaries as required by Canadian law. Party A and Party B reserve the right to decline or halt any transaction involving a digital asset that they reasonably believe may be a security, if it cannot be completed in compliance with all Applicable Laws or if doing so would require Party A or Party B to obtain a registration or license which they do not hold.

Party C agrees that it will seek its own counsel or professional advice regarding any regulatory requirements applicable to its trading of digital assets, including any securities law or exchange control requirements in its jurisdiction. Party A and Party B make no representations or

warranties as to whether any digital asset is or is not a security or regarding any legal characterization of digital assets, except that they will comply with any official determination by a competent authority.

17. Forward-Looking Statements

From time to time, communications or materials from Party A or Party B (including website content, white papers, presentations, or other disclosures) may contain forward-looking statements or information regarding their operations, plans, or future prospects. Any such forward-looking statements reflect the views or expectations of Party A or Party B (or their affiliates) as of the time made and are subject to known and unknown risks, uncertainties, and assumptions that could cause actual outcomes or results to differ materially from those expressed or implied by those statements. Words such as "believe," "expect," "anticipate," "plan," "intend," "seek," "estimate," "may," "will," "continue," and similar expressions are intended to identify forward-looking statements. However, the absence of these words does not mean that a statement is not forward-looking.

Party C acknowledges that forward-looking statements are not guarantees of future performance and should not be unduly relied upon. Neither Party A nor Party B, nor any of their affiliates, undertakes any obligation to update or revise any forward-looking statements publicly, whether as a result of new information, future events, or otherwise, except as required by applicable law or regulation.

18. Liability and Indemnification

18.1 Indemnification

Each Party (the "Indemnifying Party") agrees to indemnify, defend, and hold harmless the other Party or Parties (each an "Indemnified Party") from and against any and all losses, damages, liabilities, fines, penalties, costs, and expenses (including reasonable attorneys' fees) arising out of or resulting from any third-party claim, demand, lawsuit, regulatory investigation, or enforcement action to the extent caused by: **(i)** the Indemnifying Party's breach of this Agreement (including, but not limited to, any unauthorized use or disclosure of Confidential Information or failure to comply with data protection obligations set forth herein); **(ii)** the Indemnifying Party's violation of any Applicable Laws in relation to the activities under this Agreement; or **(iii)** the Indemnifying Party's infringement or misappropriation of any third party's intellectual property or other rights in connection with its performance under this Agreement. For example, if Party A improperly discloses a customer's Personal Data in breach of this Agreement and, as a result, the customer brings a legal claim against Party B or a regulator imposes a fine on Party B (who had shared the data in reliance on Party A's compliance), then Party A would indemnify Party B for the resulting losses and expenses. The Indemnifying Party's obligations under this section are conditioned on the Indemnified Party: (a) giving prompt written notice to the Indemnifying Party of any claim or action for which indemnity is sought (provided that failure to do so only relieves the Indemnifying Party of its obligations to the extent it is materially prejudiced by the delay); (b) allowing the Indemnifying Party to assume control of the defense and settlement of the claim (with counsel reasonably acceptable to the Indemnified Party); and (c) cooperating with the Indemnifying Party in the

defense. The Indemnifying Party shall not settle any claim in a manner that imposes any liability or admission of fault on an Indemnified Party without that Party's prior written consent, which shall not be unreasonably withheld or delayed.

18.2 Limitation of Liability

No Indirect or Consequential Damages: To the maximum extent permitted by law, no Party shall be liable to any other Party for any indirect, incidental, special, punitive, or consequential damages whatsoever, or for any loss of profit, revenue, business, goodwill, opportunity, or anticipated savings, or loss of data, arising out of or relating to this Agreement or the services provided hereunder, whether in contract, tort (including negligence), strict liability, or otherwise, and regardless of whether such damages were foreseeable or a Party was advised of the possibility of such damages.

Cap on Direct Damages: Each Party's total aggregate liability to the other Party/Parties for any and all claims arising out of or in connection with this Agreement (whether arising in contract, tort, or otherwise) shall not exceed the total fees (if any) paid by Party C to that Party under this Agreement in the six (6) months immediately preceding the event giving rise to the claim. If no fees were paid (for example, in a pure data-sharing arrangement with no monetary exchange), the Parties may agree on a nominal cap or each Party's liability shall be limited to a reasonable amount to be determined under the circumstances. This limitation applies in aggregate to all claims and causes of action of any kind.

Non-Excludable Liability: Nothing in this Agreement shall limit or exclude any Party's liability for: (i) its own fraud or willful misconduct; (ii) its infringement of the other Party's intellectual property rights; (iii) personal injury or property damage caused by its negligence to the extent such liability cannot be excluded by law; or (iv) any other liability that cannot be limited or excluded under Applicable Law.

Carve-Out for Certain Obligations: The limitations and exclusions of liability in this Section 18.2 shall not apply to breaches of Section 13 (Confidentiality) or Section 12 (Data Protection and Security) by a Party, nor to the indemnification obligations set forth in Section 18.1. In the event of such breaches or indemnifiable claims, the breaching or Indemnifying Party shall be liable for the direct losses and costs incurred by the other Party, subject to the other provisions of this Agreement and applicable law.

Several Liability: The liability of each Party under this Agreement is several and not joint. No Party shall be responsible for any liabilities or obligations incurred by any other Party, except as expressly set forth in this Agreement. If two or more Parties are found jointly liable to a third party and the third party recovers from one of them, as between the Parties the loss shall be apportioned according to each Party's relative fault.

19. Term and Termination

19.1 **Term:** This Agreement shall become effective on the Acceptance Date set forth above once executed by Party A, Party B, and Party C. It shall continue in effect until terminated in accordance with this Section 19.

19.2 **Termination by Mutual Consent:** This Agreement may be terminated at any time by the mutual written agreement of all Parties. In such event, the Parties shall jointly decide on the Acceptance Date of termination and any transition measures that may be needed (for example, how to handle any pending data requests or ongoing compliance matters at the time of termination).

19.3 **Voluntary Withdrawal by a Party:** Any Party may terminate its participation in this Agreement for convenience (i.e., without the need to show cause) by providing at least ninety (90) days' prior written notice to the other Parties of its intent to withdraw. In the case of a voluntary withdrawal by one Party, the remaining Parties shall consult during the notice period to determine whether they wish to continue a bilateral arrangement under this Agreement or terminate the Agreement entirely. For clarity, if Party C is the withdrawing Party, this Agreement may either be terminated entirely or, if Party A and Party B anticipate adding a new Party C, kept in place for that purpose. If Party A or Party B withdraws and only two Parties remain, they may choose to continue a bilateral service and data-sharing relationship by amending this Agreement accordingly. On the Acceptance Date of a Party's withdrawal, that Party shall cease to be bound by (or benefit from) the ongoing provisions of this Agreement (except for those obligations that survive termination), and the remaining Parties shall handle future data requests or services without involvement of the withdrawn Party.

19.4 **Termination for Cause:** In addition to any other rights of termination specified elsewhere in this Agreement, any Party may terminate this Agreement *in its entirety* (or, if appropriate, terminate the involvement of a particular Party) for cause upon written notice to the other Parties, upon the occurrence of any of the following events:

a. Material Breach: Another Party commits a material breach of this Agreement – including, but not limited to, a breach of confidentiality or data protection obligations, misuse of shared data, failure to comply with Applicable Laws, or a significant security lapse – and, if such breach is curable, fails to cure it within thirty (30) days after receiving written notice from the non-breaching Party describing the breach in reasonable detail. If the breach by its nature is not curable, or if the breaching Party refuses to cure or continues to breach, termination may be effective immediately upon notice. The non-breaching Party shall have the right to decide to terminate either the entire Agreement or, if practicable, to terminate only with respect to the breaching Party (in which case the breaching Party would be treated as withdrawn).

b. Legal Prohibition: A change in law or a binding order of any competent authority occurs that makes the data-sharing arrangement or the provision of services under this Agreement illegal or impossible for a Party to continue. In such a case, the affected Party must provide notice to the others with details of the legal prohibition. The Parties shall attempt in good faith to modify this Agreement or their practices to come into compliance with the law (for example, by suspending certain data transfers or adding new safeguards). If compliance or modification is not reasonably possible, the affected Party may terminate this Agreement (in whole or in part, as required) on the shortest notice necessary to comply with the law (which may be immediate, if the circumstances so require).

c. Loss of Required License or Status: If any Party loses a license, registration, or regulatory status that is material to this Agreement (for example, Party A ceases to be authorized to operate as a money services business, or Party B is subjected to regulatory sanctions that legally prohibit

it from continuing the data-sharing or service arrangement), and such status is not reinstated within a reasonable period of time, the other Party/Parties may terminate this Agreement upon written notice, either entirely or with respect to the non-compliant Party.

d. Insolvency or Bankruptcy: If any Party becomes insolvent, admits inability to pay its debts as they come due, makes a general assignment for the benefit of creditors, or if any bankruptcy, reorganization, debt arrangement, receivership, liquidation or other proceeding under bankruptcy or insolvency law is instituted by or against any Party and is not dismissed within a reasonable period (not to exceed 60 days), then another Party may terminate this Agreement effective immediately upon written notice to the insolvent Party (or as of a date specified in such notice).

19.5 **Consequences of Termination:** Upon termination of this Agreement (or upon a Party's withdrawal, in which case references below to "the Parties" apply to the terminating/withdrawing Party and each remaining Party, as the context requires):

- **(a) Cessation of Data Sharing:** The Parties shall immediately cease any ongoing or planned transfers of KYC/KYB Data under this Agreement, except to the extent that continuing a particular transfer is required by law or expressly authorized in writing by the affected data subject or by a surviving separate agreement. Any pending requests for information between the Parties that have not yet been fulfilled as of the termination Acceptance Date shall be deemed canceled, unless the Parties mutually agree in writing to fulfill certain requests during a transition period.

- **(b) Return or Destruction of Data:** The Parties shall, within a reasonable period (not to exceed sixty (60) days from the Acceptance Date of termination, or earlier if required by Section 12.10 or Section 13.6), return to the originating Party or securely destroy all Confidential Information (including Customer Due Diligence Information) received from the other Parties under this Agreement. Each Party may retain copies of data strictly as required by its internal record retention policies or Applicable Laws (for example, to satisfy regulatory record-keeping obligations), but any such retained data shall remain subject to the confidentiality and data protection provisions of this Agreement. Upon request, each Party will confirm in writing that it has completed the return/destruction of the other Party's Confidential Information, aside from any lawfully retained copies.

- **(c) Ongoing Compliance for Existing Customers:** The Parties acknowledge that termination does not retroactively undo data that was lawfully shared or services provided while the Agreement was in effect. If Party A, Party B, and Party C have common customers for whom one Party relied on another Party's KYC/KYB checks, each Party will need to ensure it can continue to meet its compliance obligations for those customers after termination. This may involve each Party independently obtaining from the customer any information that it can no longer obtain from the former partner. The Parties agree to cooperate, even after termination, in good faith to facilitate an orderly transition that avoids any non-compliance or service disruption for customers. For example, if Party A had been relying on Party B's verification of a client's identity documents, Party A may, after termination, request the client to re-submit those documents directly to Party A, or seek a one-time confirmation or copy from Party B during a brief wind-down period (if Party B is willing and legally permitted to provide it).

However, nothing in this subsection shall obligate any Party to continue sharing new or updated customer data with another Party after the Acceptance Date of termination, except as may be expressly agreed in writing for winding-down purposes.

- **(d) Survival of Terms:** Any provision of this Agreement which by its nature or explicit terms is intended to survive termination (including, but not limited to, confidentiality obligations, data protection commitments for data already exchanged, limitations of liability, indemnities, governing law and dispute resolution provisions, and any provisions regarding record-keeping or post-termination cooperation) shall survive the expiration or termination of this Agreement. All other rights and obligations of the Parties shall cease as of the effective termination date.

19.6 **Effect of Corporate Changes:** If any Party undergoes a significant corporate change (such as a merger, acquisition, or change of control) or wishes to assign its role under this Agreement to an affiliate or successor entity, such change shall be handled in accordance with the Assignment provisions of Section 21.3. Such a corporate change or assignment in itself shall not be deemed a termination of this Agreement or a cause for termination by the other Parties, unless the conditions of Section 19.4 or Section 21.3 are triggered (e.g., assignment without required consent).

(Section 19.7 is intentionally omitted.)

20. Governing Law and Dispute Resolution

20.1 **Governing Law:** This Agreement, and any disputes or claims (including non-contractual disputes or claims) arising out of or in connection with it, shall be governed by and construed in accordance with the laws of the **Republic of Panama**, without regard to its conflict of laws principles. Each Party agrees that the governing law choice in this Section 20.1 shall not be deemed to override any mandatory local law requirements applicable to that Party's handling of data or performance under this Agreement, but the laws of Panama will govern the interpretation, validity, and enforcement of the contractual terms herein.

20.2 **Initial Dispute Resolution – Good Faith Negotiation:** If any dispute, controversy, or claim arises between the Parties out of or relating to this Agreement, or the breach, termination, or validity thereof (a "Dispute"), the Parties shall first attempt in good faith to resolve the Dispute informally. A Party raising a Dispute shall provide written notice to the other Parties describing the nature of the issue in reasonable detail. Promptly after such notice is delivered, each Party shall designate a senior representative (for example, a senior executive or director who has not been directly involved in the matter) to meet (in person or via teleconference) and negotiate in good faith toward a resolution. If the Parties' senior representatives are unable to resolve the Dispute within thirty (30) days from the date of the initial notice (or such longer period as the Parties may mutually agree in writing), then the Dispute may be escalated as described in Section 20.3 below.

20.3 **Arbitration:** If a Dispute is not resolved through the informal negotiation process outlined in Section 20.2, the Dispute shall be finally resolved by binding arbitration. The arbitration shall be administered by the Centro de Conciliación y Arbitraje de Panamá (Panama Conciliation and Arbitration Center) of the Chamber of Commerce, Industries and Agriculture of Panama, and

conducted in accordance with its Commercial Arbitration Rules. There shall be one (1) arbitrator, unless the Parties agree in writing to a panel of three arbitrators due to the complexity or value of the dispute. The arbitrator(s) shall be impartial and shall be appointed in accordance with the applicable rules of the arbitration center. The seat or legal place of arbitration shall be Panama City, Republic of Panama. The arbitration proceedings shall be conducted in the English language, and any documents not in English shall be accompanied by an English translation. The arbitrator shall have the authority to award any relief that a court of competent jurisdiction could order under the Agreement and applicable law, including monetary damages (subject to the limitations in this Agreement) and injunctive or specific performance relief. The arbitral award shall be made in writing and shall state the reasons upon which it is based. The award shall be final and binding on all Parties, and judgment on the award may be entered by any court having jurisdiction.

20.4 **Interim Relief:** Notwithstanding the agreement to arbitrate, each Party retains the right to seek interim, emergency, or conservatory measures at any time from a court of competent jurisdiction (or, if available, from an emergency arbitrator under the arbitration rules) to prevent immediate and irreparable harm. This includes, for example, temporary restraining orders or preliminary injunctions to prevent a breach of confidentiality or misuse of Personal Data or other Confidential Information. Seeking such interim relief shall not be deemed a waiver of the obligation to arbitrate the underlying Dispute, and the Parties agree that the arbitrator once appointed shall have the same power to order interim measures as any court, to the extent allowed by the arbitration rules.

20.5 **Confidentiality of Proceedings:** The Parties agree that any negotiations pursuant to Section 20.2 and all aspects of any arbitration proceeding (including hearings, evidence, filings, and awards) shall be kept confidential and shall not be disclosed to any third party, except (i) to the extent necessary to enforce an arbitral award or to pursue an appeal (if permitted) of an arbitral award in court, (ii) as required by law or regulatory authority (subject to any protective orders or confidentiality arrangements that may be available), or (iii) to the Parties' respective legal counsel, accountants, or insurers, who shall be bound to keep such information confidential. The Parties further agree that any arbitration under this Agreement shall be conducted on an **individual, bilateral basis** only. There shall be no right or authority for any Dispute to be arbitrated or litigated on a class, collective, or consolidated basis, or on behalf of the general public or any other entities or persons not a Party to this Agreement.

20.6 **Costs:** Each Party shall bear its own attorneys' fees and other costs of preparing and presenting its case in any dispute resolution proceeding under this Section 20, except as otherwise provided in Section 18 or if the arbitrator or court (as applicable) awards such fees and costs to the prevailing party. The arbitrator's fees and any administrative fees for the arbitration shall be borne equally by the Parties, unless the arbitrator in the final award determines a different allocation is appropriate due to the circumstances (for example, in the event a claim is found to be frivolous or a Party acted in bad faith, the arbitrator may award costs and fees against that Party).

20.7 **Continued Performance:** Pending the final resolution of any Dispute (whether through negotiation, arbitration, or court proceeding), the Parties shall continue to perform their undisputed obligations under this Agreement, unless the performance of such obligations is

objectively impossible or impracticable under the circumstances. The existence of a Dispute shall not, in itself, relieve any Party from its duty to perform its remaining obligations under this Agreement. For example, the Parties must continue to maintain confidentiality and data security measures and honor ongoing service commitments that are not subject to the Dispute, except to the extent that the subject of the Dispute directly precludes performance.

21. General Provisions

21.1 **Entire Agreement:** This Agreement, including any annexes or schedules attached hereto (which are hereby incorporated by reference), constitutes the entire understanding and agreement between the Parties with respect to the subject matter herein (namely, the provision of services to Party C and the sharing of KYC/KYB/Customer Due Diligence Information among the Parties). It supersedes all prior or contemporaneous discussions, agreements, negotiations, proposals, and communications, whether oral or written, between the Parties relating to the same subject matter. Each Party acknowledges that, in entering into this Agreement, it is not relying on any representation, warranty, promise, or statement that is not expressly set out in this Agreement.

21.2 **Amendments:** No amendment, modification, or waiver of any provision of this Agreement shall be effective unless it is made in a written document approved by authorized representatives of Party A and Party B and communicated to Party C through the website, platform, or other electronic means. Party C's continued access to or use of the services after such amendment becomes effective shall constitute acceptance of the amended terms. This requirement includes any amendment to add a new party to this Agreement or to modify obligations due to changes in law. For the avoidance of doubt, informal communications such as emails or verbal discussions shall not constitute an amendment or waiver of any term of this Agreement unless and until they are formalized in accordance with this Section.

21.3 **Assignment:** No Party may assign, transfer, or novate this Agreement or any of its rights or obligations hereunder to any third party (whether by operation of law or otherwise) without the prior written consent of the other Parties, except that: **(i)** Party A or Party B may, upon written notice to the other Parties, assign its rights and obligations under this Agreement to an affiliate or to a successor entity in the event of a corporate reorganization, merger, or sale of substantially all of its assets or business, provided that the assignee agrees in writing to be bound by all terms of this Agreement and assumes all obligations of the assigning Party; and **(ii)** Party C, if it is undergoing a corporate reorganization or change of control, may also assign this Agreement to its successor with the prior consent of Party A and Party B (such consent not to be unreasonably withheld) and with a written assumption of obligations by the assignee. Any attempted assignment in violation of this Section 21.3 shall be null and void and of no effect. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the Parties and their respective successors and permitted assigns. *(For clarity, a change of control of a Party (through stock purchase or otherwise) shall not be deemed an assignment by that Party, but the Party undergoing the change of control shall remain obligated to ensure the new controlling persons abide by the terms of this Agreement.)*

21.4 **No Waiver:** No failure or delay by any Party in exercising any right, power, or remedy under this Agreement shall operate as a waiver thereof, nor shall any single or partial exercise of

any right, power, or remedy preclude any further or future exercise of that or any other right, power, or remedy. **Any waiver** of any provision or right under this Agreement must be in writing and signed by the Party granting the waiver. A written waiver of a breach of one provision shall not be deemed to be a waiver of any other provision or of any subsequent breach of the same provision.

21.5 **Severability:** If any provision of this Agreement (or portion thereof) is held to be invalid, illegal, or unenforceable by a court or arbitral tribunal of competent jurisdiction, that provision (or portion) shall be deemed modified to the minimum extent necessary to make it valid and enforceable, or if such modification is not possible, it shall be severed from this Agreement. In either case, the remaining provisions of this Agreement shall remain in full force and effect. The Parties shall negotiate in good faith to replace any invalid or unenforceable provision with a valid and enforceable provision that, to the greatest extent possible, achieves the original intent and economic effect of the invalid provision.

21.6 **No Third-Party Beneficiaries:** This Agreement is intended for the sole and exclusive benefit of the signatory Parties and their permitted successors and assigns. Nothing in this Agreement is intended to confer any rights, legal or equitable, in any person or entity that is not a Party to this Agreement. In particular, notwithstanding any data protection laws that might give individuals rights regarding their Personal Data, no customer or other third party shall be deemed a third-party beneficiary of this Agreement for purposes of contract enforcement. *(This clause does not negate any rights individuals may have under applicable data protection laws; it merely clarifies that this Agreement does not give external parties any contractual rights or claims.)*

21.7 **Notices:** Any formal notice or other communication required or permitted to be given under this Agreement shall be in writing and shall be deemed properly given and effective upon receipt when delivered: **(i)** by hand or by internationally recognized courier service, with proof of delivery; **(ii)** by registered or certified mail (airmail if international), return receipt requested, postage prepaid; or **(iii)** by email, **provided** that a copy is also sent by one of the foregoing methods (i) or (ii). Notices shall be sent to the addresses (and email addresses) of the Parties set forth at the beginning of this Agreement, or to such other address/email as a Party may designate by written notice to the others in accordance with this Section. A notice delivered by hand or courier is effective on the date of delivery as indicated by the signed delivery receipt. A notice sent by registered/certified mail is effective on the fifth business day after mailing (or the tenth business day if mailed internationally). A notice sent by email (with confirmation of transmission) is effective on the date the recipient's email system shows it was received (if sent during the recipient's normal business hours) or on the next business day (if sent outside normal business hours). The Parties agree that routine operational communications (such as day-to-day data requests or service inquiries) may be conducted via ordinary business email or through secure portals between designated contacts, but any formal notice invoking rights or remedies (such as notices of breach, termination, indemnifiable claim, or legal dispute) must be delivered in accordance with this Section 21.7.

21.8 **Counterparts and Electronic Signatures:** This Agreement may be executed in multiple counterparts, each of which shall be deemed an original, and all counterparts together shall constitute one and the same instrument. Signatures delivered by facsimile, email (as a PDF attachment), or by other electronic/digital signature method (e.g., via a recognized e-signature

platform) shall be deemed valid and binding for all purposes. The Parties agree that electronic signatures (whether digital certificates or other forms of e-signature) are intended to authenticate this Agreement and shall have the same legal effect as hand-written signatures.

21.9 **Headings:** The section and subsection headings (and any table of contents) in this Agreement are for convenience of reference only and shall not affect the construction or interpretation of any provision of this Agreement. Unless otherwise expressly stated, the words "including" or "include" shall be read to mean "including, without limitation," and references to any law or regulation shall be construed as including all statutory and regulatory provisions consolidating, amending, or replacing the law or regulation.

21.10 **Language:** This Agreement is executed in the English language, which shall be the governing language for all purposes. If this Agreement is translated into another language, the English version shall prevail to the extent of any conflict or ambiguity. All communications and notices made or given pursuant to this Agreement shall be in the English language, unless otherwise agreed by the Parties in writing.

21.11 **Further Assurances:** Each Party shall, at its own cost and expense, execute and deliver such documents and perform such acts as may be reasonably required to give full effect to this Agreement and to carry out the intent of the Parties. This includes, but is not limited to, the Parties cooperating in good faith to obtain any regulatory approvals or to make any notifications that may be required for their data-sharing arrangement, and updating internal procedures or agreements as necessary to align with the commitments made herein.

21.12 **Force Majeure:** No Party shall be liable for any failure or delay in performing its obligations (other than payment obligations) under this Agreement if such failure or delay is caused by circumstances beyond its reasonable control, and without the fault or negligence of the affected Party. Such circumstances include, but are not limited to, acts of God, flood, fire, earthquake, epidemic or pandemic, war, terrorism, civil unrest, governmental actions or orders, embargoes, strikes or labor disputes (not including strikes of a Party's own employees), failures or fluctuations in electrical power or telecommunications service, or outages of the internet or other communications networks not caused by the Party. The Party affected by a force majeure event shall promptly notify the other Parties of the event, describing its impact on performance, and make reasonable efforts to mitigate the effects of the event. If the force majeure event continues for an extended period (e.g., more than sixty (60) days), the Parties will discuss in good faith appropriate modifications to this Agreement (including possible termination) to fairly address the situation.

21.13 **Change of Control:** In the event that Party A or Party B undergoes a change of control (for example, through a merger with or acquisition by a third-party entity), such Party shall have the right to transfer or assign all customer information and data it has collected (including Customer Due Diligence Information pertaining to Party C) to the successor or acquiring entity as part of that transaction, **provided** that the successor agrees to be bound by confidentiality and data protection obligations no less strict than those set forth in this Agreement. Party A or Party B (whichever is undergoing the change of control) shall give notice to the other Parties as soon as reasonably practicable about the transaction (to the extent not prohibited by law or confidentiality restrictions) and the proposed transfer of data. Party C acknowledges that such transfers of information may occur in the context of a merger, acquisition, sale of business, or

other change of control, and that following such transfer, Party C's relationship may continue with the new entity under the terms of this Agreement (unless otherwise renegotiated). All provisions of this Agreement that by their nature extend beyond termination – including those related to data use, confidentiality, dispute resolution, and general provisions – shall survive any completion of a change of control transaction. A change of control as described in this Section 21.13 shall be deemed a permitted assignment of this Agreement by Party A or Party B (as applicable) pursuant to Section 21.3.

21.14 *(Intentionally omitted.)*

By clicking "I Agree" the Client confirms that it has read, understood, and agrees to be legally bound by this Agreement.

If the Client is acting on behalf of an entity, the individual accepting this Agreement represents that they have authority to bind that entity.

Annex A: Platform Terms and Conditions

The following additional terms apply to Party C's use of Party A's or Party B's online platforms, websites, or related services (collectively, the "Site") in connection with the services under the Agreement. These terms are incorporated into the Agreement, and Party C (as a user of the Site) agrees to comply with them:

A1. Intellectual Property and Acceptable Use

All content, features, and functionality on the Site – including without limitation all text, software, code, scripts, graphics, images, logos, trademarks, service marks, videos, and other materials – are owned by Party A or Party B (as applicable), or their licensors or content providers, and are protected by intellectual property laws. Party C acknowledges that Party A and Party B (and/or their affiliates) retain all proprietary rights in the Site and its contents, including the company names, logos, product and service names, and associated slogans.

Party C is granted a limited, non-exclusive, non-transferable, revocable license to access and use the Site and its content **for Party C's internal business purposes** and solely in connection with the services provided under the Agreement. Party C **shall not** reproduce, distribute, modify, create derivative works of, publicly display, publicly perform, republish, download or store (except for page caching), or transmit any of the material on the Site, except as permitted in writing by Party A or Party B or as automatically enabled by the Site's sharing features. The following are permissible uses by Party C: (i) Party C may temporarily download or cache copies of Site materials as needed to view content via a web browser; (ii) if the Site includes social media sharing features or links, Party C may take actions that are enabled by those features (consistent with any additional terms of the third-party platforms); and (iii) any other use that Party A or Party B expressly authorizes in writing. Any use of the Site not expressly permitted is strictly prohibited and may violate intellectual property and other laws. Party C agrees not to remove or alter any copyright, trademark, or other proprietary rights notices from copies of materials downloaded or printed from the Site.

Party C shall **not** access or use any part of the Site or services or materials available through the Site for any commercial purpose other than the transactions and business contemplated by the Agreement. If Party C breaches any term of this Section A1 or otherwise uses the Site in violation of the Agreement or applicable law, Party A or Party B may immediately terminate or suspend Party C's access to the Site, and delete or deactivate Party C's related accounts or data, without prior notice and without liability. Such suspension or termination shall be in addition to any other remedies available to Party A or Party B.

A2. Account Security

Party C is responsible for obtaining its own hardware, software, and internet access needed to use the Site, and for ensuring that any persons who access the Site through Party C's internet connection or credentials are aware of and comply with the Agreement's terms. Certain areas or features of the Site may require Party C to register for an account or provide information. When registering, Party C agrees to provide truthful, current, and complete information. Party C is responsible for maintaining the confidentiality of its account credentials (such as usernames, passwords, API keys, or multi-factor authentication devices) and for all activities that occur

under Party C's account. **Party C agrees to immediately notify Party A or Party B** (whichever operates the relevant Site or service) of any suspected unauthorized access to or use of Party C's account or any other breach of security.

Party A and Party B implement physical, electronic, and administrative measures to secure Personal Data and account information; however, Party C understands that no transmission of information via the internet is completely secure or error-free, and no system is entirely immune to compromise. **Accordingly, Party A and Party B do not guarantee absolute security** of information transmitted through the Site. Party C provides information at its own risk and is responsible for using appropriate security measures (such as up-to-date antivirus software and secure networks) when accessing the Site. Except to the limited extent required by applicable law, Party A and Party B shall not be liable for any unauthorized access to or alteration of Party C's transmissions or data, any material or data sent or received or not sent or received, or any transactions entered into through the Site. Party C hereby waives any claims against Party A and Party B related to unauthorized access, alteration, destruction, or disclosure of Party C's data, except to the extent caused by Party A's or Party B's violation of the express terms of the Agreement.

Party C agrees not to violate or attempt to violate the security of the Site, including by (i) accessing data or content not intended for Party C, or logging into a server or account which Party C is not authorized to access; (ii) attempting to probe, scan, or test the vulnerability of the Site or any related system or network, or to breach security or authentication measures, without proper authorization; (iii) interfering or attempting to interfere with service to any user, host, or network (such as by submitting a virus to the Site, overloading, "flooding," "spamming," or "crashing"); or (iv) injecting malicious code, scripts, or automated agents (like bots) in a manner that disrupts or compromises the Site's functionality. Any such violations may result in immediate termination of access to the Site and potential legal action.

A3. Conditions of Use and Content Standards

By accessing and using the Site, Party C agrees to use it only for lawful purposes and in accordance with the Agreement. Party C also agrees to ensure that any and all content, material, or information that Party C or its agents submit, post, publish, display, or transmit on or through the Site (collectively, "User Submissions") complies with the following content standards. **User Submissions** must not:

- **Violate Laws:** Violate any Applicable Laws or regulations, or contain any material that could give rise to civil or criminal liability under applicable law or regulations.
- **Violate Third-Party Terms:** Violate the terms of service of any third-party website linked to or integrated with the Site. For example, if the Site allows posting via a third-party social media platform, the content must not violate that platform's terms.
- **Abusive or Objectionable Content:** Contain or promote anything exploitative, obscene, pornographic, sexually explicit, excessively violent, harassing, hateful, or discriminatory (including on the basis of race, sex, religion, nationality, disability, sexual orientation, or age, or any other legally prohibited ground), or otherwise be **objectionable** as determined in Party A's or Party B's sole discretion.

- **Harm to Individuals:** Involve stalking, harassing, or exploiting any individual (especially minors) in any way, or seek or provide information that violates any person's privacy or personal security.
- **False or Misleading Information:** Provide false, misleading, or fraudulent information (for instance, impersonating any person or entity, or misrepresenting Party C's affiliation with a person or entity).
- **Impersonation:** Impersonate Party A, Party B, any of their employees, another user, or any other person or entity, or imply an affiliation with them without authorization.
- **Illegal Activity:** Promote or advocate any illegal activity or unlawful act.

Party A and Party B reserve the right (but assume no obligation) to remove or refuse to post any User Submission that violates these standards or the terms of the Agreement, and to take any appropriate measures (including legal action or referral to law enforcement) in response to any violation.

A4. User Submissions and License Grant

Party C acknowledges that any User Submissions it provides through the Site will **not** be treated as confidential or proprietary by Party A or Party B (except for personal information protected by privacy laws, which will be handled as described in the Agreement and applicable Privacy Policies). By providing any User Submission on or through the Site, Party C grants Party A, Party B, and their affiliates, service providers, and each of their respective licensees, successors, and assigns a worldwide, royalty-free, perpetual, irrevocable, non-exclusive right and license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, perform, and display such material (in whole or in part) and to incorporate it in other works in any form, media, or technology, without compensation to Party C. Party C also **waives any moral rights** or rights of attribution in that content, to the extent permitted by law. This license and waiver enable Party A and Party B to process and utilize the content (for example, any feedback or ideas submitted) for any purpose consistent with providing and improving services.

By submitting any content, Party C represents and warrants that it owns or controls all necessary rights in and to the content and has the right to grant the license above to Party A and Party B. Party C further represents that all such User Submissions do and will comply with the **Content Standards in Section A3** of this Annex and all other provisions of the Agreement. Party C is fully responsible for any User Submissions it provides and for any consequences thereof, including any third-party claims. Party A and Party B are not responsible or liable to any third party for the content or accuracy of any User Submissions posted by Party C (or any other user of the Site).

A5. Service Availability and Updates

Party A and Party B each reserve the right to modify, suspend, or discontinue, whether temporarily or permanently, any part of their Site or services at any time without prior notice. Party C agrees that neither Party A nor Party B will be liable to Party C or any third party for any modification, suspension, unavailability, or discontinuation of any online service, content, or

feature. While Party A and Party B will aim to provide Party C with reasonable notice of major changes when feasible, they are under no obligation to do so for routine or emergency updates. Any new features or updates that augment or enhance the current services shall be subject to this Agreement.

Party C understands that the Site (or certain features) may occasionally be unavailable due to scheduled maintenance, emergency repairs, telecommunications interruptions, or other circumstances beyond Party A's or Party B's control. Party A and Party B will not be responsible for any loss or inconvenience to Party C due to the Site's unavailability.

A6. Jurisdictional Restrictions

Party C shall ensure that its access and use of the Site and services complies with all laws and regulations applicable to Party C in its jurisdiction. Information provided via the Site, or any services or products described, are not intended for distribution or use by any person or entity in any jurisdiction or country where such distribution or use would be contrary to law or regulation, or which would subject Party A or Party B to any registration or licensing requirement within such jurisdiction that they do not already hold. Party A and Party B each reserve the right to limit the availability of the Site or services, in whole or in part, to any person, geographic region, or jurisdiction, at any time and in their sole discretion. By accessing or using the Site, Party C represents and warrants that doing so does not violate any laws or regulations applicable to Party C, including those regarding export control, sanctions, or restrictions on the use of encryption technologies.

If Party C is located in or is a national of a country that is subject to trade sanctions, embargoes, or other legal restrictions (e.g., listed by FATF as non-cooperative or by any government as a sanctioned jurisdiction), Party C is not authorized to use or access the Site or services unless explicitly permitted by all relevant authorities. Any offer of services on the Site is void where prohibited. Party C shall promptly notify Party A and Party B if at any time Party C becomes subject to any restriction or change in status (for example, being listed on a sanctions list) that would impact Party C's ability to legally use the services.