

BTC – USDT PROGRAM OPERATING PROCEDURE

Programs with BTC and USDT starting at €1,000,000

Initial program: 3 months, extendable up to 12 months

Reference asset: BTC / USDT

Minimum Reference Capital: €1,000,000 or equivalent in BTC/USDT

Indicated target return: up to 20% weekly, subject to operating conditions, strategy, liquidity and contractual documentation

Brokerage fee: 3%

Commission distribution: 50% / 50% among the corresponding commission agents/intermediaries.

Important notice: The performance figures stated herein constitute proposed trading objectives or conditions and should not be construed as guaranteed profitability. Any transaction must be subject to due diligence, risk analysis, party verification, regulatory compliance and written contract.

1. Subject matter of the proceedings

This procedure establishes a methodology for the evaluation, verification and eventual incorporation of capital in BTC and USDT trading programs aimed at participants with a minimum reference capital of €1,000,000 or equivalent.

The main objective is to establish a transparent process that allows:

- 🏛️ Identify and verify the participating parties.
- 🏛️ Verify the existence and operational availability of assets.
- 🏛️ Determine who maintains custody of the funds.
- 🏛️ Avoid unnecessary transfers of the owner's assets.
- 🏛️ Establish a verifiable mechanism to prove certain transactions on the blockchain.
- 🏛️ Clearly define the economic conditions, commissions, duration and responsibilities.
- 🏛️ Maintain documentary traceability of all actions.

2. Duration of the program

The programme is initially planned for a period of 3 months, with the possibility of extension up to a maximum of 12 months, provided that:

- 🏛️ The parties agree.
- 🏛️ Contractual conditions are met.
- 🏛️ Liquidity and operational conditions are maintained.
- 🏛️ Compliance and due diligence controls are passed.
- 🏛️ There are no legal, regulatory, technical or counterparty incidents.
- 🏛️ Any extension must be formalized in writing before the end of the current period.

3. Custody of the owner's assets

As a fundamental principle of the procedure:

The owner's BTC or USDT shall not be transferred or placed under the control of third parties unless there is a specific contractual agreement, a duly verified custody structure, and the corresponding legal safeguards.

The mere incorporation of the owner into the process does not imply that they must hand over their private keys, seed phrase, exchange credentials, 2FA codes or any mechanism that allows them to take control of their assets.

In no case will the following be requested:

- 🏛️ Seed phrase.
- 🏛️ Private key.
- 🏛️ Password.
- 🏛️ 2FA code.
- 🏛️ Remote access to the wallet.
- 🏛️ Screenshots that reveal sensitive information.
- 🏛️ Information that allows the security of the account to be compromised.
- 🏛️ The ownership and custody of the funds must be clearly identified before starting any operation.

4. Verification of funds and wallet control

In the context of cryptocurrencies, blockchain provides public mechanisms to verify certain operations.

A transaction hash (TXID) is a public identifier associated with a transaction recorded on a blockchain. It allows you to locate and check a transaction using the corresponding explorer, for example, Etherscan for certain Ethereum operations or Tronscan for transactions on TRON.

This is especially useful because:

- 🏠 A screenshot can be manipulated.
- 🏠 A video can be manipulated.
- 🏠 A balance displayed within an exchange may not amount to self-custodial funds.
- 🏠 An internal transfer from an exchange may not result in a public transaction on the blockchain.
- 🏠 An alleged A → B transfer may need independent verification.
- 🏠 The TXID can be checked, depending on the network and browser:
 - 🏠 The issuing address.
 - 🏠 The receiving address.
 - 🏠 The amount transferred.
 - 🏠 The date and time of the operation.
 - 🏠 The confirmation status.
 - 🏠 The network used.
 - 🏠 The block in which the operation was registered.
- 🏠 Therefore, the hash is an objective tool to verify that a certain transaction was recorded on a public blockchain network.

5. Does sharing a TXID compromise security?

Under normal conditions, sharing only the TXID of a transaction does not provide access to funds.

The TXID is a public identifier and does not contain:

- 🏠 The private key.
- 🏠 The seed phrase.
- 🏠 The password.
- 🏠 Access credentials.
- 🏠 The ability to sign new transactions.
- 🏠 Nonetheless, a blockchain transaction can reveal public information such as:
 - 🏠 Addresses involved.
 - 🏠 Amount transferred.
 - 🏠 Observable history of those addresses.
 - 🏠 Approximate time of the operation.

For this reason, the TXID should be considered public traceability information, not a security credential.

6. Operational Control Test

It is important to distinguish between proof of funds and proof of control of a direction.

The mere display of a balance does not necessarily demonstrate that the reporting person is able to dispose of those funds.

Where operational control is required, a limited, pre-agreed test may be used, for example:

- 🏠 Determine a small test quantity.
- 🏠 Identify the corresponding blockchain network.
- 🏠 Perform a controlled transaction.
- 🏠 Get the TXID.
- 🏠 Check the TXID in the public browser.
- 🏠 Confirm the addresses and amount.
- 🏠 Record the result in documentation.

Where technically possible, an even more conservative alternative is to use message signing mechanisms or equivalent cryptographic procedures, avoiding moving funds.

The test should be performed only with small quantities and under previously agreed instructions.

7. What does hash actually validate?

The TXID mainly validates that a particular transaction has been included and recorded on the corresponding blockchain.

When a test is properly designed, it can help verify operational capability over a direction. However, an isolated TXID does not by itself prove:

- ⌚ The legal identity of the owner.
- ⌚ The total solvency of the owner.
- ⌚ The definitive economic ownership of all the funds.
- ⌚ The absence of obligations or encumbrances on assets.
- ⌚ The future ability to maintain the same balance.
- ⌚ The legitimacy of a given investment strategy.

As such, the TXID should be part of a broader due diligence process.

8. Why request a blockchain proof?

The main purpose is to reduce counterparty risk.

Among the risks that are intended to be avoided are:

- ⌚ Balances shown via screenshots.
- ⌚ View-only wallets.
- ⌚ Funds temporarily belonging to third parties.
- ⌚ Exchange balances without sufficient information about their availability.
- ⌚ Addresses that are not under the participant's operational control.
- ⌚ Inability to execute a trade when needed.

Blockchain proof allows a subjective statement to be replaced by a piece of data that can be independently checked on the network.

9. Relationship with traditional banking instruments

In traditional financial transactions, there are messaging and banking documentation mechanisms, such as certain SWIFT communications and other instruments used by financial institutions.

In blockchain, verifying a transaction works differently.

It should not be claimed that a TXID is legally equivalent to banking instruments such as MT799, MT760 or MT700. They are different mechanisms, with different purposes and legal frameworks.

The TXID does provide verifiable technical evidence of a particular transaction:

- ⌚ Unique identifier.
- ⌚ Public Registry.
- ⌚ Information about sender and receiver.
- ⌚ Amount.
- ⌚ Inclusion in blockchain.
- ⌚ Confirmation status according to the network.

10. Incorporation procedure

Phase 1 — Identification

The necessary information will be collected from the parties:

- ⌚ Identification of persons or entities.
- ⌚ Corporate information, when applicable.
- ⌚ Beneficial owner.
- ⌚ Origin of funds.
- ⌚ Necessary banking or financial information.
- ⌚ Relevant blockchain addresses.

Step 2 — Due diligence

Prior to any operation, a reasonable assessment shall be made of:

- ▣ Identity of the parties.
- ▣ Origin and legitimacy of the funds.
- ▣ Counterparty risk.
- ▣ Regulatory risk.
- ▣ Risk of sanctions.
- ▣ AML/KYC risk.
- ▣ Technological risk.
- ▣ Custody risk.
- ▣ Liquidity risk.

Phase 3 — Blockchain Verification

Addresses will be checked and, where appropriate, a limited operational control test will be requested. The test should use small quantities and should not require the delivery of private keys or credentials.

Phase 4 — Contract

Before starting the operation, there must be a contract that determines, at least:

- ▣ Capital.
- ▣ Assets used.
- ▣ Duration.
- ▣ General strategy.
- ▣ Risks.
- ▣ Case.
- ▣ Performance objectives.
- ▣ Commissions.
- ▣ Distribution of commissions.
- ▣ Liquidation procedure.
- ▣ Conditions of termination.
- ▣ Responsibilities of each party.
- ▣ Applicable Jurisdiction.
- ▣ Compliance procedures.

Phase 5 — Initiation

Once the verifications have been completed and the contract signed, the operation can begin in accordance with the agreed conditions.

11. Performance and Economic Conditions

The program contemplates a commercial performance target of up to 20% per week.

This figure should be treated as a condition or objective subject to the strategy and the actual results of the operation, and not as a guaranteed return.

The parties must expressly establish:

- ▣ Whether the yield is gross or net.
- ▣ If it is calculated on initial capital or compound capital.
- ▣ Settlement periodicity.
- ▣ Loss treatment.
- ▣ Risk limits.
- ▣ Reinvestment conditions.
- ▣ Right of withdrawal.
- ▣ Treatment of negative periods.

A return of 20% per week implies an extraordinarily high level of risk if it is to be sustained and therefore any commercial presentation must avoid misleading about the nature and risk of the operation.

12. Commissions

The total expected commission is 3%, with distribution:

- ▣ 50% for the first commission agent/intermediary.
- ▣ 50% for the second commission agent/intermediary.
- ▣ This means, unless otherwise agreed:
- ▣ 1.50% for the first commission agent.
- ▣ 1.50% for the second commission agent.
- ▣ The commissions must be expressly reflected in the contract and specify:
- ▣ Basis on which it is calculated.
- ▣ Moment of devengo.
- ▣ Time of payment.
- ▣ Payment currency or asset.
- ▣ Party responsible for payment.
- ▣ Corresponding tax treatment.

13. Safety Principles

No participant must submit:

- ▣ Seed phrase.
- ▣ Private key.
- ▣ Password.
- ▣ 2FA code.
- ▣ Recovery code.
- ▣ Remote access to devices.
- ▣ Exchange credentials.

The verification must be carried out using public information and appropriate cryptographic mechanisms. Where a test transfer is required, it must be of limited amount, pre-authorised and documented.

14. Traceability

Each operation must be able to be related to sufficient documentation to reconstruct the process later.

It is recommended to keep:

- ▣ Date and time.
- ▣ Address of origin.
- ▣ Destination address.
- ▣ Network used.
- ▣ Amount.
- ▣ TXID.
- ▣ Blockchain explorer used.
- ▣ Identification of the operation.
- ▣ Corresponding contractual documentation.

The information shall be stored securely and in accordance with applicable legal and data protection obligations.

15. Principle of transparency

Trust in a cryptocurrency trade should not be based exclusively on documents, screenshots, business presentations, or verbal statements.

The combination of: identification + due diligence + contract + blockchain verification + traceability + clear custody provides a much stronger basis for evaluating a trade.

The TXID is a technical verification tool, but it is not a substitute for legal, financial, regulatory, or counterparty analysis.

16. Conclusion

In a transaction with BTC and USDT, the blockchain allows certain transactions to be independently verified without the need to rely exclusively on a declaration from the parties.

The TXID:

- ▣ It is a public identifier.
- ▣ It allows you to locate a transaction.
- ▣ It allows you to check your registration on the blockchain.
- ▣ Facilitates independent verification.
- ▣ It does not itself provide access to funds.

As such, it can be used as a piece of an operational control verification procedure.
However, it should not be presented as a guarantee of solvency, profitability or legitimacy of an investment.
The incorporation of a capital of €1,000,000 or more must be conditional on the identification of the parties, verification of the origin of the funds, due diligence, contractual review, risk assessment and compliance with applicable regulations.

Fundamental rule of procedure:

No private keys or seed phrases are requested. Profitability is not guaranteed. Screenshots are not considered sufficient.
Any relevant transaction must be verifiable by independent evidence and contractually documented.

PROCEDIMIENTO OPERATIVO PROGRAMA BTC – USDT

Programas con BTC y USDT a partir de 1.000.000 €

Programa inicial: 3 meses, ampliable hasta 12 meses

Activo de referencia: BTC / USDT

Capital mínimo de referencia: 1.000.000 € o equivalente en BTC/USDT

Rendimiento objetivo indicado: hasta un 20 % semanal, sujeto a condiciones operativas, estrategia, liquidez y documentación contractual

Comisión de intermediación: 3 %

Distribución de comisiones: 50 % / 50 % entre los comisionistas/intermediarios correspondientes.

Aviso importante: Las cifras de rendimiento indicadas en este documento constituyen objetivos o condiciones comerciales propuestas y no deben interpretarse como una rentabilidad garantizada. Cualquier operación deberá estar sometida a due diligence, análisis de riesgo, verificación de las partes, cumplimiento normativo y contrato escrito.

1. Objeto del procedimiento

El presente procedimiento establece una metodología para la evaluación, verificación y eventual incorporación de capital en programas de operativa con BTC y USDT destinados a participantes con un capital mínimo de referencia de 1.000.000 € o equivalente.

El objetivo principal es establecer un proceso transparente que permita:

- Identificar y verificar a las partes participantes.
- Verificar la existencia y disponibilidad operativa de los activos.
- Determinar quién mantiene la custodia de los fondos.
- Evitar transferencias innecesarias de los activos del propietario.
- Establecer un mecanismo verificable para demostrar determinadas operaciones en blockchain.
- Definir claramente las condiciones económicas, comisiones, duración y responsabilidades.
- Mantener trazabilidad documental de todas las actuaciones.

2. Duración del programa

El programa se plantea inicialmente por un período de **3 meses**, con posibilidad de ampliación hasta un máximo de **12 meses**, siempre que:

- Las partes estén de acuerdo.
- Se cumplan las condiciones contractuales.
- Se mantengan las condiciones de liquidez y operatividad.
- Se superen los controles de compliance y due diligence.
- No existan incidencias legales, regulatorias, técnicas o de contraparte.

Cualquier ampliación deberá formalizarse por escrito antes de finalizar el período vigente.

3. Custodia de los activos del propietario

Como principio fundamental del procedimiento:

Los BTC o USDT del propietario no deberán ser transferidos ni puestos bajo control de terceros salvo que exista un acuerdo contractual específico, una estructura de custodia debidamente verificada y las garantías legales correspondientes.

La mera incorporación del propietario al proceso no implica que deba entregar sus claves privadas, seed phrase, credenciales de exchange, códigos 2FA ni ningún mecanismo que permita tomar el control de sus activos.

En ningún caso se solicitará:

- Seed phrase.
- Clave privada.
- Contraseña.
- Código 2FA.
- Acceso remoto a la wallet.
- Capturas que revelen información sensible.
- Información que permita comprometer la seguridad de la cuenta.

La titularidad y custodia de los fondos deberán quedar claramente identificadas antes de comenzar cualquier operativa.

4. Verificación de fondos y control de wallet

En el contexto de criptomonedas, la blockchain proporciona mecanismos públicos para verificar determinadas operaciones.

Un **transaction hash (TXID)** es un identificador público asociado a una transacción registrada en una blockchain. Permite localizar y comprobar una operación mediante el explorador correspondiente, por ejemplo, Etherscan para determinadas operaciones sobre Ethereum o Tronscan para operaciones sobre TRON.

Esto resulta especialmente útil porque:

- Un screenshot puede ser manipulado.
- Un vídeo puede ser manipulado.
- Un saldo mostrado dentro de un exchange puede no equivaler a fondos autocustodiados.
- Una transferencia interna de un exchange puede no generar una transacción pública en blockchain.
- Una supuesta transferencia A → B puede necesitar verificación independiente.

Mediante el TXID pueden comprobarse, según la red y el explorador:

- La dirección emisora.
- La dirección receptora.
- El importe transferido.
- La fecha y hora de la operación.
- El estado de confirmación.
- La red utilizada.
- El bloque en el que quedó registrada la operación.

Por tanto, el hash constituye una herramienta objetiva para verificar que **una determinada transacción fue registrada en una red blockchain pública**.

5. ¿Compartir un TXID compromete la seguridad?

En condiciones normales, compartir únicamente el TXID de una transacción no proporciona acceso a los fondos.

El TXID es un identificador público y no contiene:

- La clave privada.
- La seed phrase.
- La contraseña.
- Las credenciales de acceso.
- La capacidad de firmar nuevas transacciones.

No obstante, una transacción blockchain puede revelar información pública como:

- Direcciones implicadas.
- Importe transferido.
- Historial observable de esas direcciones.
- Momento aproximado de la operación.



Por este motivo, el TXID debe considerarse **información pública de trazabilidad**, no una credencial de seguridad.

6. Prueba de control operativo

Es importante distinguir entre **prueba de fondos** y **prueba de control de una dirección**.

La simple visualización de un saldo no demuestra necesariamente que la persona que presenta la información pueda disponer de esos fondos.

Cuando sea necesario acreditar control operativo, podrá utilizarse una prueba limitada y previamente acordada, por ejemplo:

- Determinar una cantidad de prueba pequeña.
- Identificar la red blockchain correspondiente.
- Realizar una transacción controlada.
- Obtener el TXID.
- Verificar el TXID en el explorador público.
- Confirmar las direcciones y el importe.
- Registrar documentalmente el resultado.

Cuando técnicamente sea posible, una alternativa todavía más conservadora consiste en utilizar mecanismos de **firma de mensaje** o procedimientos criptográficos equivalentes, evitando mover fondos.

La prueba deberá realizarse únicamente con cantidades pequeñas y bajo instrucciones previamente acordadas.

7. ¿Qué valida realmente el hash?

El TXID valida principalmente que **una transacción concreta ha sido incluida y registrada en la blockchain correspondiente**.

Cuando una prueba se diseña adecuadamente, puede contribuir a verificar la capacidad operativa sobre una dirección. Sin embargo, un TXID aislado no demuestra por sí mismo:

- La identidad jurídica del titular.
- La solvencia total del propietario.
- La titularidad económica definitiva de todos los fondos.
- La ausencia de obligaciones o gravámenes sobre los activos.
- La capacidad futura de mantener el mismo saldo.
- La legitimidad de una determinada estrategia de inversión.

Por ello, el TXID debe formar parte de un proceso de due diligence más amplio.

8. ¿Por qué solicitar una prueba blockchain?

La finalidad principal es reducir el riesgo de contraparte.

Entre los riesgos que se pretende evitar se encuentran:

- Saldos mostrados mediante capturas de pantalla.
- Wallets de solo visualización.
- Fondos pertenecientes temporalmente a terceros.
- Saldos de exchanges sin información suficiente sobre su disponibilidad.
- Direcciones que no están bajo control operativo del participante.
- Imposibilidad de ejecutar una operación cuando sea necesario.

La prueba blockchain permite sustituir una afirmación subjetiva por un dato que puede ser comprobado independientemente en la red.

9. Relación con instrumentos tradicionales de banca

En operaciones financieras tradicionales existen mecanismos de mensajería y documentación bancaria, como determinadas comunicaciones SWIFT y otros instrumentos utilizados por entidades financieras.

En blockchain, la verificación de una transacción funciona de manera diferente.

No debe afirmarse que un TXID sea jurídicamente equivalente a instrumentos bancarios como MT799, MT760 o MT700. Son mecanismos distintos, con finalidades y marcos jurídicos diferentes. El TXID sí proporciona una evidencia técnica verificable de una transacción concreta:

- Identificador único.
- Registro público.
- Información sobre emisor y receptor.
- Importe.
- Inclusión en blockchain.
- Estado de confirmación según la red.

10. Procedimiento de incorporación

Fase 1 — Identificación

Se recopilará la información necesaria de las partes:

- Identificación de las personas o entidades.
- Información societaria, cuando corresponda.
- Beneficiario efectivo.
- Origen de los fondos.
- Información bancaria o financiera necesaria.
- Direcciones blockchain relevantes.

Fase 2 — Due diligence

Antes de cualquier operación se realizará una evaluación razonable de:

- Identidad de las partes.
- Origen y legitimidad de los fondos.
- Riesgo de contraparte.
- Riesgo regulatorio.
- Riesgo de sanciones.
- Riesgo AML/KYC.
- Riesgo tecnológico.
- Riesgo de custodia.
- Riesgo de liquidez.

Fase 3 — Verificación blockchain

Se comprobarán las direcciones y, cuando proceda, se solicitará una prueba limitada de control operativo.

La prueba deberá utilizar cantidades pequeñas y no deberá requerir la entrega de claves privadas ni credenciales.

Fase 4 — Contrato

Antes de iniciar la operación deberá existir un contrato que determine, como mínimo:

- Capital.
- Activos utilizados.
- Duración.
- Estrategia general.
- Riesgos.
- Custodia.
- Objetivos de rendimiento.
- Comisiones.
- Distribución de comisiones.
- Procedimiento de liquidación.
- Condiciones de terminación.
- Responsabilidades de cada parte.
- Jurisdicción aplicable.
- Procedimientos de compliance.

Fase 5 — Inicio

Una vez completadas las verificaciones y firmado el contrato, podrá iniciarse la operativa conforme a las condiciones acordadas.

11. Rendimiento y condiciones económicas

El programa contempla comercialmente un **objetivo de rendimiento de hasta el 20 % semanal**.

Esta cifra deberá tratarse como una condición u objetivo sujeto a la estrategia y a los resultados reales de la operativa, y **no como una rentabilidad garantizada**.

Las partes deberán establecer expresamente:

- ▣ Si el rendimiento es bruto o neto.
- ▣ Si se calcula sobre capital inicial o capital compuesto.
- ▣ Periodicidad de liquidación.
- ▣ Tratamiento de pérdidas.
- ▣ Límites de riesgo.
- ▣ Condiciones de reinversión.
- ▣ Derecho de retirada.
- ▣ Tratamiento de períodos negativos.

Una rentabilidad del 20 % semanal implica un nivel de riesgo extraordinariamente elevado si se pretende mantener de forma sostenida, por lo que cualquier presentación comercial deberá evitar inducir a error sobre la naturaleza y el riesgo de la operación.

12. Comisiones

La comisión total prevista es del **3 %**, con distribución:

- ▣ 50 % para el primer comisionista/intermediario.
- ▣ 50 % para el segundo comisionista/intermediario.

Esto supone, salvo pacto diferente:

- ▣ 1,50 % para el primer comisionista.
- ▣ 1,50 % para el segundo comisionista.

Las comisiones deberán quedar reflejadas expresamente en el contrato y especificar:

- ▣ Base sobre la que se calcula.
- ▣ Momento de devengo.
- ▣ Momento de pago.
- ▣ Moneda o activo de pago.
- ▣ Parte responsable del pago.
- ▣ Tratamiento fiscal correspondiente.

13. Principios de seguridad

Ningún participante deberá entregar:

- ▣ Seed phrase.
- ▣ Private key.
- ▣ Contraseña.
- ▣ Código 2FA.
- ▣ Código de recuperación.
- ▣ Acceso remoto a dispositivos.
- ▣ Credenciales de exchange.



La verificación deberá realizarse utilizando información pública y mecanismos criptográficos apropiados. Cuando sea necesario realizar una transferencia de prueba, deberá ser de importe limitado, estar previamente autorizada y quedar documentada.

14. Trazabilidad

Cada operación deberá poder relacionarse con documentación suficiente para reconstruir posteriormente el proceso. Se recomienda conservar:

-  Fecha y hora.
-  Dirección de origen.
-  Dirección de destino.
-  Red utilizada.
-  Importe.
-  TXID.
-  Explorador blockchain utilizado.
-  Identificación de la operación.
-  Documentación contractual correspondiente.

La información deberá almacenarse de forma segura y de acuerdo con las obligaciones legales y de protección de datos aplicables.

15. Principio de transparencia

La confianza en una operación con criptomonedas no debe basarse exclusivamente en documentos, capturas de pantalla, presentaciones comerciales o declaraciones verbales.

- La combinación de: **identificación + due diligence + contrato + verificación blockchain + trazabilidad + custodia clara** proporciona una base mucho más sólida para evaluar una operación.
- El TXID es una herramienta de verificación técnica, pero no sustituye el análisis jurídico, financiero, regulatorio o de contraparte.

16. Conclusión

En una operativa con BTC y USDT, la blockchain permite verificar de manera independiente determinadas transacciones sin necesidad de confiar exclusivamente en una declaración de las partes.

El TXID:

-  Es un identificador público.
-  Permite localizar una transacción.
-  Permite comprobar su registro en la blockchain.
-  Facilita la verificación independiente.
-  No proporciona por sí mismo acceso a los fondos.

- Por ello, puede utilizarse como una pieza de un procedimiento de verificación de control operativo. Sin embargo, **no debe presentarse como una garantía de solvencia, rentabilidad o legitimidad de una inversión.** La incorporación de un capital de 1.000.000 € o superior deberá quedar condicionada a la identificación de las partes, verificación del origen de los fondos, due diligence, revisión contractual, evaluación de riesgos y cumplimiento de la normativa aplicable.

Regla fundamental del procedimiento:

No se solicitan claves privadas ni seed phrases. No se garantiza una rentabilidad. No se consideran suficientes las capturas de pantalla. Toda operación relevante debe poder verificarse mediante evidencias independientes y quedar documentada contractualmente.



TERMS AND CONDITIONS OF USE **TERMS AND CONDITIONS OF USE 1. ACCEPTANCE, VALIDITY, AND ENTIRE AGREEMENT** Please read these Terms and Conditions carefully. By accessing this website (<https://bank-to-bank.es>) and its pages, you acknowledge that you have read, understood, and agree to be bound by these Conditions of Use, the legal notice, the cookie policy, and any other specific instructions or conditions communicated to you. If you do not agree, please leave the site immediately. The **BANK-TO-BANK CONSORTIUM** business group reserves the



right to modify these terms at any time without prior notice, in exercise of its unilateral modification power permitted by Article 5 of Act 7/1998, of April 13, on General Conditions of Contracting, provided that such modification does not adversely affect rights already acquired by the user. Your continued use constitutes acceptance of such changes. This document constitutes the entire agreement between the group and the user, replacing any prior communication or understanding, by virtue of Articles 1254, 1258, and 1261 of the Spanish Civil Code, which establish the requirements and binding force of contracts. A printed version of these conditions shall be admissible in judicial or administrative proceedings, in accordance with Article 27 of Act 34/2002, of July 11, on Information Society Services and Electronic Commerce (**LSI-CE**). In the event of a conflict between these general conditions and the specific conditions of a particular service, the latter shall prevail, according to the principle of normative specialty. **2. IDENTIFICATION OF THE OWNER** (Compliance with Art. 10 **LSI-CE**) In compliance with Article 10 of Act 34/2002 (**LSI-CE**), you are informed that the owner of the website is: Corporate Name: **BANK-TO-BANK CONSORTIUM** Email: bank-to-bank@bank-to-bank.es Phone: **+34 625 209 869 / +34 636 080 420** **3. PURPOSE AND SCOPE OF APPLICATION** These General Conditions regulate the access, navigation, and use of the website (<https://bank-to-bank.es>) as well as the services and content hosted thereon. They are considered General Conditions of Contracting for the purposes of the provisions of Act 7/1998, of April 13, on

General Conditions of Contracting, and Royal Legislative Decree 1/2007, of November 16, approving the Consolidated Text of the General Law for the Defense of Consumers and Users and other complementary laws (**TRLGDCU**). **4. CONDITIONS OF USE AND USER OBLIGATIONS** The user undertakes to use the website in accordance with the law, these conditions, morality, public order, and generally accepted practices. The following is expressly prohibited: Engaging in unlawful activities or acts contrary to good faith. Introducing or disseminating computer viruses or any other physical or logical system that may cause damage to the owner's or third parties' systems (classified as a crime under Article 264 et seq. of the Spanish Criminal Code). Attempting to access, use, or manipulate the data of the owner or third-party users without authorization. The user guarantees that the information provided is truthful and assumes responsibility for communicating any changes to it, in accordance with the principle of contractual good faith (Article 7 of the Civil Code). **5. PROTECTION OF PERSONAL DATA** The processing of users' personal data shall be strictly governed by: Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016 (**GDPR**). Organic Law 3/2018, of December 5, on Personal Data Protection and Guarantee of Digital Rights (**LOPDGDD**). The user expressly consents to the processing of their data for the purposes described in the Privacy Policy available on the website, and may exercise their rights of access, rectification, erasure, objection, restriction of processing, and data portability at any time by directing a request to the email address indicated in Section 2, or by filing a claim with the Spanish Data Protection Agency (**AEPD**). **6. INTELLECTUAL AND INDUSTRIAL PROPERTY** All content on the website (texts, photographs, graphics, images, icons, technology, software, links, and other audiovisual or sound content, as well as its graphic design and source codes) are the intellectual property of **BANK-TO-BANK CONSORTIUM** or of third parties who have authorized their use, and are protected by Royal Legislative Decree 1/1996, of April 12, approving the Consolidated Text of the Intellectual Property Law (**LPI**), and by international treaties signed by Spain. Their reproduction, distribution, public communication, or transformation is prohibited without the express and written authorization of the owner, except for the user's personal and private use, in accordance with the limitations established in Articles 31 et seq. of the **LPI**. Trademarks, trade names, or distinctive signs are protected by Act 17/2001, of December 7, on Trademarks. **7. EXCLUSION OF WARRANTIES AND LIABILITY** **BANK-TO-BANK CONSORTIUM** shall not be liable, in any case, for damages and losses of any nature that may be caused, including but not limited to: errors or omissions in the content, lack of availability of the portal, or the transmission of viruses or malicious or harmful programs in the content, despite having adopted all necessary technological measures to prevent it, in accordance with the "lex artis" or "professional standard" of the sector. This limitation of liability applies within the limits permitted by Article 117 of the **TRLGDCU** and Article 17 of the **LSI-CE**, and shall in no case affect the non-waivable rights of consumers and users recognized by current legislation, especially in the event of willful misconduct or gross negligence on the part of the owner. **8. LINKS TO THIRD-PARTY WEBSITES** The website may contain links to third-party websites. These links are exclusively for informational purposes and do not imply that **BANK-TO-BANK CONSORTIUM** approves or recommends the content, products, or services of such sites. The owner assumes no responsibility for the content, accuracy, or privacy policies of third-party websites, in accordance with the provisions of Article 17.2 of the **LSI-CE**. **9. MODIFICATION OF CONDITIONS AND DURATION** The owner reserves the right to make, without prior notice, any modifications it deems appropriate on its portal, and may change, remove, or add both the content and services provided through the web, as well as the manner in which they are presented or located. However, such modifications shall not have retroactive effect on contracts already perfected, guaranteeing the principle of legal certainty (Article 9.3 of the Spanish Constitution). **10. APPLICABLE LAW AND JURISDICTION** For the resolution of all disputes or issues related to this website or the activities developed therein, Spanish legislation shall apply, to which the parties expressly submit. If the user has the status of a consumer or end-user: The Courts and Tribunals of the consumer's domicile shall have jurisdiction to resolve any dispute, in accordance with the provisions of Article 52 of Act 1/2000, of January 7, on Civil Procedure (**LEC**), and Article 90 of the **TRLGDCU**, which prohibit jurisdiction submission clauses to a forum other than that of the consumer in adhesion contracts. If the user is a company or professional: Both parties submit, with express waiver of any other jurisdiction that may correspond to them, to the Courts and Tribunals of the city of [City of the company's registered office, e.g., Madrid], unless mandatory law provides otherwise. **11. ONLINE DISPUTE RESOLUTION (ODR PLATFORM)** By virtue of Article 14 of Regulation (EU) No 524/2013, of May 21, on online dispute resolution in consumer matters, consumers are informed that the European Commission provides an online dispute resolution platform (**ODR Platform**), which can be accessed via the following link: <http://ec.europa.eu/consumers/odr/>. This platform serves as an entry point for the out-of-court resolution of online disputes arising from sales or service contracts concluded between a consumer and a professional.

INFORMATIONAL NATURE AND GENERAL DISCLAIMER **INFORMATIONAL NATURE AND GENERAL DISCLAIMER 2.1. PURELY INFORMATIONAL AND EDUCATIONAL NATURE** The information, data, analyses, opinions, and content available on this website are exclusively for informational, educational, and general reference purposes. They do not constitute, nor should they be interpreted in any case as, a commercial offer, a solicitation of funds, an invitation to invest, or a personalized recommendation to buy or sell securities, financial instruments, or investment products. This content is intended for companies, investors, and individuals seeking to expand their knowledge about financial information, financing structures, monetization programs, business strategies, or market opportunities. **2.2. NO PROFESSIONAL ADVICE** Nothing published on this website should be considered as personalized financial, legal, tax, accounting, or investment advice. The information presented does not take into account the specific objectives, financial situation, or particular needs of any user or entity. Before making any financial or investment decision, or before participating in any program described, the user must consult with their own professional, legal, and tax advisors to evaluate

the risks and suitability of such actions. **2.3. ACCURACY, COMPLETENESS, AND TIMELINESS** Although we strive to provide high-quality information from sources considered reliable, we do not guarantee the accuracy, completeness, timeliness, or reliability of the data, statistics, or reports presented. The materials may describe features of sample services, products, or institutions without any guarantee and are subject to daily changes due to market volatility and economic conditions. Services, products, and information are provided "as is," "as available," and "as obtained," without representation or warranty of any kind. **2.4. DISCLAIMER OF WARRANTIES** The user expressly agrees that the use of the information and services on this website is at their own and exclusive risk. All warranties, whether express or implied, are hereby expressly disclaimed, including, but not limited to, implied warranties of title, non-infringement of third-party rights, merchantability, or fitness for a particular purpose. **2.5. LIMITATION OF LIABILITY** In no event shall the owners, administrators, employees, or affiliates of this website be liable for any direct, indirect, incidental, consequential, special, exemplary, or punitive damages, including, without limitation, loss of profits, funds, data, use, goodwill, or other intangible losses, resulting from: (i) the use or inability to use the services or information; (ii) any error, omission, or inaccuracy in the content; (iii) any decision made by the user based on the information provided on this site; or (iv) any other matter related to the access to or use of this website. **2.6. THIRD-PARTY LINKS AND CONTENT** This website may contain links to third-party websites or user-generated content. Such links are provided solely for your convenience and do not necessarily imply affiliation, endorsement, or approval of such content by us. We assume no responsibility whatsoever for the content, privacy policies, practices, or availability of third-party sites.

REGULATORY STATUS, SCOPE OF ACTIVITIES, AND LIMITATIONS (CNAE 6619) 3.1. LEGAL FRAMEWORK AND EXCLUSION FROM REGISTRATION WITH SUPERVISORY BODIES



The operating entities of this website conduct their activities under the epigraph of **CNAE 6619** (Spanish National Classification of Economic Activities): *"Other activities auxiliary to financial services, except insurance and pension funds"*. Although this code encompasses heterogeneous support services for the sector, it is expressly, explicitly, and repeatedly stated that the group's companies **ARE NOT REGISTERED OR ENROLLED WITH THE NATIONAL SECURITIES MARKET COMMISSION (CNMV)**, nor with the **BANK OF SPAIN** as credit institutions, financial credit establishments, payment institutions, or electronic money institutions. Consequently, it is strictly prohibited to interpret our market presence as that of a regulated financial entity, brokerage, dealer, or Virtual Asset Service Provider (**VASP**). **3.2. STRICT DELIMITATION OF SERVICES PROVIDED** Our activity is exclusively limited to auxiliary, administrative, technological, or generic **B2B** (Business-to-Business) consulting services. Under no circumstances do we provide personalized financial advice, discretionary or continuous portfolio management, nor do we act as intermediaries in the contracting of regulated investment products (in accordance with **MiFID II** / relevant national financial regulations). The services we provide, in an enumerative but not exhaustive manner, are strictly confined to: **BACK-OFFICE AND ADMINISTRATIVE PROCESSING**: Operational support, document management, and administrative tasks delegated by third parties. **TECHNOLOGICAL PAYMENT PROCESSING**: Acting exclusively as a technological provider (SaaS, APIs, payment gateways) for the operational settlement of digital payments. At no point does the operating entity

have legal availability or custody of the end-users' funds (no third-party accounts). **ADMINISTRATIVE MANAGEMENT AND CLAIMS**: Assistance in processing, claiming, and managing taxes, fees, or refunds before public bodies, acting strictly as administrative representatives and not as financial or tax advisors. **GENERIC AND EDUCATIONAL FINANCIAL CONSULTING**: Issuance of reports, market analyses, or training materials of a strictly informative and educational nature. **NO CONTENT PUBLISHED ON THIS WEBSITE OR ISSUED BY OUR COMPANY SHALL BE INTERPRETED AS AN INVESTMENT RECOMMENDATION, PUBLIC OFFERING, OR INVITATION TO BUY/SELL FINANCIAL ASSETS.** **TECHNOLOGICAL AND DATA SUPPORT**: Provision of data analysis tools, commercial scoring, or technological infrastructure for the sector. **COLLECTION AND DEBT RECOVERY MANAGEMENT**: Management of defaults and overdue collections, acting strictly as authorized agents, without assuming credit risk or debt subrogation under any circumstances. **3.3. CURRENT OPERATIONAL STATUS: "STAND-BY" PHASE** Currently, and as part of a strategic restructuring of our business model, the two operating companies are in a **"STAND-BY" OR GENERAL COMMERCIAL INACTIVITY** status. This implies that the website is merely corporate, informative, and serves as a technological showcase. There are no active processes for onboarding new retail clients or raising funds. The entities' operations are restrictively and exclusively limited to the provision of highly specialized B2B consulting services, namely: **COMMERCIAL RISK CONSULTING**: Analysis of solvency, viability, and counterparty risk in commercial transactions. **DUE DILIGENCE (KYC/AML) ADVISOR FOR INTERNATIONAL TRADE**: Verification of corporate identities, prevention of money laundering, and regulatory compliance applied exclusively to the supply chain and physical trade of goods. **MANAGEMENT AND COMPLIANCE CONSULTING FOR COMMODITIES COMPANIES**: Advisory services on traceability, customs regulations, and regulatory frameworks applicable to the trade of raw materials, without intervening in the financial trading or derivatives of such assets. **3.4. LIMITATION OF LIABILITY AND USER'S DUTY** Given the auxiliary and unregulated nature of our activities, the operating entity disclaims any and all liability for investment decisions that users may make based on the information provided on this portal. Users, clients, and visitors are strongly urged to always verify the regulatory status of any entity they intend to do business with through the official registers of the **CNMV** or the **BANK OF SPAIN**, and to seek independent, duly qualified financial, tax, or legal advice before making any economic decisions.

DUE DILIGENCE (KYC/AML), INFORMATION VERIFICATION, DISCLAIMER REGARDING PUBLIC DATA, AND CONSEQUENCES OF NON-COMPLIANCE 4.1. SCOPE AND DEPTH OF DUE DILIGENCE

The user acknowledges, accepts, and expressly consents that all documentation, data, statements, and information provided to the consortium, or gathered during the business relationship, will be subject to a rigorous, exhaustive, and ongoing Due Diligence and Know Your Customer (**KYC**) process. This process, aligned with the strictest international standards for Anti-Money Laundering (**AML**) and Countering the Financing of Terrorism (**CFT**), includes, but is not limited to: Review, verification, and cross-referencing of information with public and private databases, commercial registries, property registries, and tax records. Verification against international sanctions lists (**OFAC, EU, UN, ETC.**), lists of Politically Exposed Persons (**PEPs**), and their close associates and family members. Screening in national and international media, social networks, and **OPEN SOURCE INTELLIGENCE (OSINT)** sources for the detection of adverse media. Identification and verification of the Ultimate Beneficial Owner (**UBO**) of any legal structure, trust, or entity represented by the user. **4.2. NATURE OF INFORMATION AND THE "MIRROR PRINCIPLE"** The user accepts and understands that the **BANK-TO-BANK CONSORTIUM** acts solely as a collector, aggregator, and processor of information that is already in the public domain or generated by third parties. The consortium is not the creator, modifier, auditor, or guarantor of the absolute accuracy, integrity, or currency of such third-party records. The consortium is limited to applying the "mirror principle," that is, mirroring and reflecting the objective and public reality existing at the time of consultation. Therefore, any error, obsolescence, or inaccuracy in the original public data is not attributable to the consortium. **4.3. ABSOLUTE DISCLAIMER OF LIABILITY AND INDEMNIFICATION** Consequently, if the user disagrees with the results, conclusions, risk ratings, or reports derived from this verification process, they expressly, voluntarily, knowingly, and irrevocably waive the right to file any type of claim, lawsuit, complaint, or legal action, whether of a civil, commercial, criminal, or administrative nature, against the consortium, its member entities, administrators, employees, auditors, or affiliates. Furthermore, the user undertakes to hold harmless and indemnify the consortium against any claims, damages, or losses



that may arise from third parties due to the communication or processing of this public data by the consortium in compliance with its legal obligations. **4.4. REPUTATIONAL RISK, PUBLIC RECORDS, AND EXCLUSION OF THE "RIGHT TO BE FORGOTTEN"** The consortium assumes no responsibility whatsoever for any harm, detriment, moral damage, or impact on the user's image, reputation, honor, or commercial credit that may arise from the existence, accessibility, cross-referencing, or disclosure of such public records, litigation, or debts. The user expressly declares that, as this involves information of a public nature and legally accessible, processed for compliance with legal obligations and the exercise of the consortium's legitimate interest, **THEY ARE NOT ENTITLED TO AND CANNOT EXERCISE THE RIGHTS OF ERASURE ("RIGHT TO BE FORGOTTEN") OR RESTRICTION OF PROCESSING** regarding such data within the consortium's systems. The safeguarding of one's own image, the correction of errors in source registries, and the clearing of public records are the sole, non-transferable, and exclusive responsibility of the user. **4.5. CONSEQUENCES OF DISCREPANCIES, OMISSIONS, OR FALSEHOODS** The user guarantees that all information provided is truthful, current, and complete. In the event that the Due Diligence process reveals discrepancies, deliberate omissions, documentary falsehoods, or an unacceptable risk profile for the consortium, the consortium reserves the absolute right and discretion to: Reject the application or deny the requested operation without the need for extensive justification. Immediately suspend or terminate any business relationship or operational account. Retain funds or documents in preventive custody according to applicable regulations. File a Suspicious Activity Report (**SAR**) or report to the Financial Intelligence Unit (**FIU**) or competent authority, without this generating any liability for the consortium towards the user. **4.6. DATA RETENTION, GDPR, AND REGULATORY COMPLIANCE** Finally, in exercise of the legitimate interest recognized in Article 6.1(f) of Regulation (**EU**) 2016/679 (**GDPR**), and in strict compliance with legal obligations regarding the prevention of money laundering (Article 6.1(c) **GDPR**), the consortium will retain all documentation, evidence, Due Diligence reports, and communication trails provided or generated by the user. This retention will be maintained for the legally established statute of limitations periods (which in AML matters is typically a minimum of 10 years following the termination of the business relationship). This retention has the sole and exclusive purpose of prevention, investigation, and the filing or exercise of possible judicial or extrajudicial claims, the defense of the consortium's interests, and the demonstration of regulatory compliance (accountability) before supervisory authorities.

LEGAL REPRESENTATION, PARTNER IDENTITY AND DISCLAIMER OF LIABILITY FOR THIRD-PARTY ACTIONS **5.1. ACCREDITATION OF PARTNER AND REPRESENTATIVE STATUS** Only those natural or legal persons who are expressly listed as such in the public deeds of incorporation or modification thereof, duly registered with the corresponding Commercial Registry, shall have the legal status of partners, administrators, attorneys-in-fact or legitimate representatives of the companies that make up the **BANK-TO-BANK CONSORTIUM** business group. Representative capacity shall be strictly governed by the provisions of said public titles and current commercial legislation. **5.2. INEFFECTIVENESS OF ACTIONS BY UNAUTHORIZED THIRD PARTIES** Any person who, not appearing in said official documentation, claims, declares or presents themselves to third parties as a partner, representative, employee, collaborator, advisor or affiliate of the consortium, absolutely lacks legitimacy, legal capacity and powers of representation to bind these companies in any way. Consequently, the **BANK-TO-BANK CONSORTIUM** business group disclaims and rejects all responsibility, whether civil, criminal, commercial, administrative or labor, for any action, promise, agreement, communication, offer, negotiation or transaction that said unauthorized person attempts to carry out or has carried out in the name of the consortium. Obligations and commitments shall only be valid, enforceable and binding if formalized in writing in official documents and signed by the legal representatives duly authorized according to the current public deeds. **5.3. DIGITAL COMMUNICATIONS, SOCIAL MEDIA AND ELECTRONIC MEANS** It is expressly established that communications made through e-mails with unofficial domains, instant messaging (such as WhatsApp, Telegram or Signal), social media or websites not verified as official corporate channels, do not generate any legal bond. The consortium is not responsible for information, offers or requirements disseminated through these unofficial means by third parties. **5.4. INTERMEDIARIES, BROKERS AND EXTERNAL MANAGERS** The **BANK-TO-BANK CONSORTIUM** business group does



not maintain exclusivity agreements, nor does it grant implicit powers of representation to brokers, financial intermediaries, finders or external managers, unless there is a specific and current notaries mandate that accredits it as such. Any commission, fee or management expense demanded by these third parties from clients or investors is the sole responsibility of whoever collects it, with the consortium being totally disconnected from said economic demands. **5.5. CORPORATE IMAGE PROTECTION AND ANTI-FRAUD POLICY** Any unauthorized use of the trademarks, logos, stationery, seals, corporate name or corporate materials of **BANK-TO-BANK CONSORTIUM** will be considered a violation of intellectual and industrial property rights, as well as an act of unfair competition and/or fraud. Likewise, third parties are informed that the consortium **DOES NOT REQUEST, NOR AUTHORIZE ANYONE TO REQUEST**, advance payments, "management fees", "release fees", "bonds" or "account opening costs" for the formalization of legitimate financial or commercial operations. Any requirement of this nature made by a supposed representative is indicative of a fraudulent maneuver. **5.6. DUTY OF DILIGENCE, VERIFICATION AND OFFICIAL COMPLAINT CHANNEL** Users, clients and third parties are strongly urged to exercise the maximum duty of diligence and to verify in a reliable manner the identity and powers of representation of any interlocutor who claims to act on behalf of the consortium, requesting the relevant accrediting documentation (such as current registry certification compulsed copy of powers of attorney or official letter of appointment). To facilitate this task and report any irregularity, the following official verification and complaint channel of the business group is enabled: **E-MAIL: bank-to-bank@bank-to-bank.es** **CONTACT TELEPHONES: +34 625 209 869 / +34 636 080 420** **5.7. ABSOLUTE NULLITY AND FALSITY OF APPARENT DOCUMENTATION** It is declared expressly, categorically and unequivocally that **ANY DOCUMENT, CERTIFICATE, EMPLOYMENT CONTRACT, LETTER OF APPOINTMENT OR DEED THAT ATTEMPTS TO ATTRIBUTE TO A PERSON THE STATUS OF ATTORNEY-IN-FACT, WORKER, EMPLOYEE OR PARTNER OF BANK-TO-BANK CONSORTIUM IS ABSOLUTELY FALSE**, when said person does not appear in the official records previously mentioned. The business group **DOES NOT RECOGNIZE ANY VALIDITY, EFFECTIVENESS OR LEGITIMACY OF SAID DOCUMENTS**, and formally states that **THERE IS NO RECORD OF HAVING SIGNED, GRANTED, AUTHORIZED, SEALED OR ENDORSED ANY DOCUMENT OF THIS NATURE** in favor of unauthorized third parties. The exhibition, presentation or use of such documents by any individual will be considered a serious and sufficient indication of documentary falsity, fraud and identity theft, immediately activating all corresponding criminal and civil legal actions by the consortium. Any attempt at identity theft, documentary falsity, phishing or fraudulent representation will be immediately reported to the competent judicial, police and regulatory authorities, with the consortium reserving the right to exercise all legal actions that correspond for the claim of damages and losses, including loss of profits.

GEOGRAPHICAL RESTRICTIONS, REGULATORY COMPLIANCE (KYC/AML), AND DUE DILIGENCE The Consortium carefully selects its clients and reserves the right of admission, not accepting all business requests. Our policy is one of zero tolerance towards illicit operations; therefore, all proposals and transactions must strictly comply with international Anti-Money Laundering (**AML**) and Counter-Terrorist Financing (**CFT**) laws. **6.1. FATCA RESTRICTIONS AND PROHIBITED JURISDICTIONS** Due to the Foreign Account Tax Compliance Act (**FATCA**) and the Consortium's internal regulations, **NO SERVICES ARE PROVIDED TO U.S. passport holders, U.S. incorporated entities, U.S. tax residents, or clients using U.S. based or**



U.S. correspondent banks for transaction processing. Furthermore, operations involving jurisdictions classified as non-cooperative tax havens or countries subject to international trade embargoes are strictly rejected. **6.2. REGULATORY FRAMEWORK AND INTERNATIONAL STANDARDS** All operations are governed by strict compliance with: **EU Directive 91/308/EEC**, and its successive amendments and updates (including Directives **2001/97/EC**, **2005/60/EC**, and the most recent **EU AML Directives**). The 40 Recommendations of the Financial Action Task Force (**FATF**). United Nations conventions against drug trafficking, transnational organized crime, and corruption. Guidelines of the Basel Committee on Banking Supervision. Consolidated sanctions lists of the European Union, **OFAC** (Office of Foreign Assets Control), and the **UN Security Council**. **6.3. KNOW YOUR CUSTOMER (KYC) DUE DILIGENCE AND ULTIMATE BENEFICIARIES** The Consortium applies Know Your Customer (**KYC**) and Enhanced Due Diligence (**EDD**) policies. It is mandatory to identify and verify the **ULTIMATE BENEFICIAL OWNER (UBO)** of any corporate entity, tracing down to the natural persons holding final control of the company. Additionally, thorough screening is conducted to identify Politically Exposed Persons (**PEPs**) and their close family members or associates, requiring senior management approval to operate with such profiles. **6.4. VERIFICATION OF COMMERCIAL AND BANKING DOCUMENTATION** Any document submitted within the framework of a transaction (including, but not limited to, **SCO**, **FCO**, **ICPO**, **LOI**, **RWA**, **BCL**, or financial instruments such as **LC**, **SBLC**, **BG**) is subject to verification. **ZERO TOLERANCE FOR FRAUD:** Any fraudulent, altered, or falsified document will be immediately rejected, the transaction will be canceled, and the incident will be reported to the competent authorities and international financial fraud databases. **GROUNDWORK FOR REJECTION:** Documentation will be discarded due to poor scan quality, lack of authorized signatures, absence of official bank stamps, suspected forgery, data inconsistencies, or failure to meet the technical specifications required by the Consortium. **BANK VERIFICATION:** Financial capacity documents (**BCL**, **RWA**) and payment instruments must be verified directly from bank to bank (**BANK-TO-BANK**) through secure systems such as **SWIFT (MT199/MT799)**; verifications through intermediaries or private servers will not be accepted. **6.5. CONSEQUENCES OF NON-COMPLIANCE AND CONFIDENTIALITY** Non-compliance with **AML/KYC** regulations will result in the immediate termination of negotiations and the inclusion of the offenders in the Consortium's internal blacklist. If any indications of money laundering are detected, a Suspicious Activity Report (**SAR**) will be filed with the relevant Financial Intelligence Unit (**FIU**). All information and documentation provided by the client during the **KYC** process will be treated with strict confidentiality, stored on secure servers, and used exclusively for regulatory compliance purposes, in accordance with applicable data protection laws.

INTELLECTUAL AND INDUSTRIAL PROPERTY, COPYRIGHT, AND DIGITAL ASSETS All rights, title, and interest in the website, its digital platforms, and all associated content belong exclusively to the **BANK-TO-BANK CONSORTIUM** business group or its legitimate licensors. The website and its services are intended solely for personal, informational, and non-commercial use. **7.1. OWNERSHIP AND SCOPE OF RIGHTS** The intellectual property of the Consortium encompasses, including but not limited to: the source code, graphic design, user interfaces, navigation structures, databases, texts, images, videos, icons, as well as **OPERATIONAL METHODOLOGIES, STANDARD OPERATING PROCEDURES (SOPS), FINANCIAL DOCUMENT TEMPLATES, CONTRACT TEMPLATES, AND THE CONSORTIUM'S "KNOW-HOW"**. All these elements are protected by national and international copyright, trademark, and patent laws. **7.2. LICENSE OF USE AND STRICT RESTRICTIONS** Users are granted a limited, revocable, non-exclusive, and non-transferable license to access and use the site. It is **STRICTLY PROHIBITED**, without the prior, express, and written authorization of the **BANK-TO-BANK CONSORTIUM**: The reproduction, distribution, public communication, transformation, or creation of derivative works. The use of **"FRAMING"**, **"DEEP LINKING"** techniques, or massive data extraction ("scraping" or "data mining"). Reverse engineering, decompilation, or disassembly of the source code and underlying software. The circumvention, deactivation, or interference with security measures or **DIGITAL RIGHTS MANAGEMENT (DRM)** implemented on the site. Any commercial, lucrative, or business use of the site's content or tools. **7.3. TRADEMARKS, TRADE NAMES, AND CORPORATE ASSETS** The name **"BANK-TO-BANK CONSORTIUM"**, its logo, slogans, domain names, and any other trademark or distinctive sign displayed on the site are registered or pending registration property. Unauthorized use of these trademarks, or any element that may cause confusion or discredit the Consortium, constitutes an infringement of industrial property rights and will be prosecuted by appropriate legal means. **7.4. USER-GENERATED CONTENT AND**



ASSIGNMENT OF RIGHTS In the event that users submit, upload, or transmit any content (comments, documents, data) through the site: **WARRANTY OF OWNERSHIP:** The user warrants that they are the legitimate owner of the intellectual property rights to said content and that its submission does not infringe upon the rights of third parties. **LICENSE TO THE CONSORTIUM:** The user grants the **BANK-TO-BANK CONSORTIUM** a worldwide, perpetual, irrevocable, non-exclusive, transferable, sublicensable, and royalty-free license to use, reproduce, modify, adapt, publish, translate, and distribute said content in any format, in connection with the site's services and the Consortium's operations. **WAIVER OF MORAL RIGHTS:** To the maximum extent permitted by applicable law, the user waives their moral rights over the submitted content. **INDEMNIFICATION:** The user agrees to indemnify and hold harmless the Consortium against any claims, damages, or losses arising from the infringement of third-party intellectual property rights by the content provided by the user. **7.5. SUGGESTIONS AND "FEEDBACK"** Any comments, suggestions, improvement ideas, or **"FEEDBACK"** sent by users to the Consortium shall be considered non-confidential information. The **BANK-TO-BANK CONSORTIUM** shall have absolute freedom to use, reproduce, and exploit such suggestions for any purpose, without any obligation of compensation, acknowledgment, or restriction towards the user. **7.6. INFRINGEMENTS AND LEGAL ACTIONS** Non-compliance with any of the stipulations in this section will result in the immediate revocation of the use license, permanent blocking of the user's account, and deletion of their data. The **BANK-TO-BANK CONSORTIUM** reserves the right to pursue all appropriate civil and criminal actions against infringers to claim damages and losses incurred.

RULES OF CONDUCT, ACCEPTABLE USE OF THE SITE, AND USER LIABILITY The user expressly undertakes to use the site, its services, and digital platforms in accordance with applicable law, morality, public order, and these general conditions. Use of the site implies full and unconditional acceptance of all rules of conduct established herein. **8.1. GENERAL COMMITMENTS OF THE USER** The user guarantees that they will act at all times lawfully, loyally, and in good faith, refraining from using the site for any unlawful purpose or effect, harmful to the rights and interests of third parties, or that in any way may damage, disable, overburden, deteriorate, or prevent the normal use of the site, computer equipment, or documents, contents, and files contained on any of the **BANK-TO-BANK CONSORTIUM** computer systems. **8.2. STRICTLY PROHIBITED CONDUCT** It is **STRICTLY PROHIBITED** for the user, without limitation: **UNAUTHORIZED ACCESS:** Performing unauthorized access to the site, its servers, databases, or connected systems, as well as hacking, cracking, stealing, or intercepting passwords, credentials, personal data, or confidential information of other users or the Consortium. **IMPERSONATION:** Pretending to be another person or entity (impersonation), using offensive or misleading usernames, or infringing on registered trademarks, copyrights, or trade names of third parties, as well as engaging in phishing or social engineering practices. **INFRASTRUCTURE DAMAGE:** Damaging, overburdening, deteriorating, or interfering with the functioning of the site through denial-of-service (DDoS) attacks, malicious code injection, or any other technique that compromises the availability or integrity of the platform. **SPAM AND UNSOLICITED ADVERTISING:** Sending mass mail (spam), unsolicited advertising messages, pyramid letter chains, unauthorized multi-level marketing schemes, or any form of unconsented commercial communication. **ILICIT OR HARMFUL CONTENT:**

Publishing, transmitting, disseminating, or storing illegal, defamatory, obscene, pornographic, racist, xenophobic, or discriminatory content, inciting hatred, violence, or terrorism, or that is harmful to minors or vulnerable individuals. **MALWARE TRANSMISSION:** Introducing or disseminating computer viruses, trojans, worms, logic bombs, ransomware, spyware, adware, or any other malicious or technologically harmful material. **SYSTEM MANIPULATION:** Attempting to manipulate, alter, or interfere with transaction results, verification systems, KYC/AML processes, or any security mechanism of the Consortium. **8.3. PROTECTION OF TECHNOLOGICAL INFRASTRUCTURE** The user undertakes not to use, introduce, or distribute automated tools such as bots, crawlers, spiders, scrapers, or scripts of any kind to access the site, collect data, or interact with its services without the express written authorization of the **BANK-TO-BANK CONSORTIUM**. Likewise, the use of proxies, **VPNs**, or other technologies designed to evade geographical restrictions, sanctions, or security blocks implemented by the Consortium is strictly prohibited. **8.4. ADVERTISING, BUSINESS MODEL, AND ACCEPTANCE OF COMMUNICATIONS** The site is funded wholly or partially through advertising, sponsorships, and commercial links. Therefore: The user expressly agrees to receive advertising, promotional, and commercial messages from the **BANK-TO-BANK CONSORTIUM** and its strategic partners, via email, push notifications, internal messaging, or other digital channels. The user undertakes **NOT TO USE TECHNOLOGIES, EXTENSIONS, SOFTWARE, FILTERS, OR METHODS** that block, hide, alter, or interfere with the reception and display of advertising integrated into the site, including ad-blockers, obfuscation tools, or any analogous mechanism. Non-compliance with this obligation will entitle the Consortium to restrict or deny access to the infringing user. **8.5. MONITORING, MODERATION, AND COOPERATION WITH AUTHORITIES** The **BANK-TO-BANK CONSORTIUM** reserves the right, but not the obligation, to monitor, review, moderate, edit, or remove any content, account, or user activity that, in its sole discretion, fails to comply with these rules or may be illegal, offensive, or harmful. The Consortium will fully cooperate with judicial, law enforcement, financial, and regulatory authorities in the investigation of any illicit activity, providing all information, connection logs, and traffic data legally required, without the need for prior notification to the affected user. **8.6. SUSPENSION, TERMINATION, AND CONSEQUENCES OF NON-COMPLIANCE** The **BANK-TO-BANK CONSORTIUM** reserves the right to: **TEMPORARILY OR PERMANENTLY LIMIT, SUSPEND, OR PREVENT** access to the site and its services for any user who fails to comply with these rules, without the need for prior notice or justification. **INTERRUPT THE SERVICE GENERALLY OR PARTIALLY** with a minimum notice of **15 BUSINESS DAYS**, except in cases of force majeure, urgent technical maintenance, cyberattacks, or situations posing a risk to the security of the Consortium or its users, in which case the interruption may be immediate. **DELETE ACCOUNTS AND CONTENT** that violate the rules of conduct, retaining only the information necessary for regulatory compliance, legal investigation, or liability claims. **PURSUE CIVIL AND CRIMINAL LEGAL ACTIONS** as appropriate against infringing users, claiming material and moral damages caused to the Consortium, its partners, or third parties. **INCLUDE THE INFRINGING USER** in internal and external blacklists, financial fraud databases, and default registries, communicating this to the competent authorities and other entities in the sector. **LIMITATION OF LIABILITY** It is expressly clarified that **NO CONTRACT, AGREEMENT, OR BINDING DOCUMENT OF ANY KIND IS SIGNED WITH US**, and that **NO TYPE OF INVESTMENT IS CARRIED OUT, MANAGED, OR FACILITATED** through this business group or consortium. Consequently, and given the absence of registration with the **CNMV (SPANISH SECURITIES MARKET COMMISSION)**, the consortium assumes no responsibility whatsoever related to investment decisions, capital losses, or transaction results, as these activities are completely unrelated to our operations. The consortium does not charge upfront commissions and is not responsible for unofficial emails, identity theft, or amounts sent to third parties on the users' own initiative.

Likewise, continuous, uninterrupted, or secure access to the website is not guaranteed. The consortium, its subsidiaries, executives, and suppliers shall not be liable for direct, indirect, special, consequential, or incidental damages arising from site failures, viruses, data interception, typographical errors, force majeure, or strikes. Finally, it is expressly stated that, in the event that the client decides to sign any document (with third parties or of any other nature), **IT IS THE CLIENT'S EXCLUSIVE RESPONSIBILITY TO CARRY OUT THEIR OWN DUE DILIGENCE BEFOREHAND AND INDEPENDENTLY**. We do not intervene, endorse, or assume any responsibility for such agreements.



CONFIDENTIALITY AND ELECTRONIC COMMUNICATIONS All exchanged information, as well as any discussions regarding potential transactions or business matters, is strictly private and confidential in nature. It is expressly clarified once again that none of these communications imply the offer, sale, purchase, or intermediation of registered government securities, financial instruments, or any other type of investment. Information shared between the parties, including but not limited to financial data, business strategies, corporate documents, and personal information, is deemed strictly confidential. Its disclosure, reproduction, or distribution to unauthorized third parties is strictly prohibited, except where strictly required by a competent judicial authority. All electronic communications, messages, documents, and attachments transmitted through this medium constitute private communications and are protected by the **ELECTRONIC COMMUNICATIONS PRIVACY ACT (18 U.S.C. 2510)**, as well as applicable securities, data protection, and privacy laws in the relevant jurisdictions. Any unauthorized interception, monitoring, use, copying, or illicit disclosure of these messages by unintended recipients is strictly prohibited and may be subject to appropriate legal action. In the event that you receive any communication, file, or information in error, please immediately notify the sender by replying to this message. Furthermore, you must immediately and irreversibly delete such information from your primary system, as well as from any backups, servers, or storage devices, and confirm its destruction in writing. Finally, it is understood that the mere exchange

of this confidential information does not create any contractual obligation, nor does it imply that any document will be signed with us, nor does it constitute an invitation to make any investment.

GOVERNING LAW, JURISDICTION, AND LANGUAGE These Terms of Use shall be governed by and construed in accordance with the laws of the Kingdom of Spain, without regard to its conflict of law principles. Any dispute, controversy, or claim arising out of or relating to these Terms shall be submitted exclusively to the competent courts located in Spain. By accessing this site, the user expressly waives any right to any other jurisdiction or to a trial by jury. Any claims must be filed within a strict period of one (1) year from the date the cause of action arises. In the event of any discrepancy or conflict between a translated version of these terms and the original Spanish version, the original Spanish version shall prevail. If any provision of these Terms is held to be invalid, illegal, or unenforceable, such provision shall be enforced to the maximum extent permissible by applicable law, and the remaining provisions shall remain in full force and effect.

DATA PROTECTION, COOKIES, AND CORPORATE INFORMATION The processing of your personal data, including the documentation retained for legal defense mentioned in section 4, is governed by our Privacy Policy, in accordance with Regulation **(EU) 2016/679 (GDPR)** and Organic Law **3/2018 (LOPDGDD)**, based on compliance with legal obligations and legitimate interest. The website uses technical and analytical cookies, which are configurable by the user. This website is operated by **INTERNATIONAL ASSET OPERATIONS SLU (B12710067)** and **INTERNATIONAL PURCHASE OF ASSET SL (B44510014)**. For more information, you may contact: bank-to-bank@bank-to-bank.es Last updated: JULY 22, 2026.



TAGS ETAGS, ASSETS (GENERIC): CONSORTIUM BANK-TO-BANK, BANK-TO-BANK, we sell assets, sell asset, buy assets, buy asset, we monetize assets, asset monetization, we duplicate assets, asset duplication, bullet assets, asset program, **SBLC STAND BY LETTER OF CREDIT**: we sell (**SBLC**) stand by letter of credit, sell (**SBLC**) stand by letter of credit, monetize (**SBLC**) stand by letter of credit, asset monetization (**SBLC**) stand by letter of credit, duplicate (**SBLC**) stand by letter of credit, asset duplication (**SBLC**) stand by letter of credit, bullet (**SBLC**) stand by letter of credit, program (**SBLC**) stand by letter of credit, **LC LETTER OF CREDIT**: we sell (**LC**) letter of credit, sell (**LC**) letter of credit, monetize (**LC**) letter of credit, asset monetization (**LC**) letter of credit, duplicate (**LC**) letter of credit, asset duplication (**LC**) letter of credit, bullet (**LC**) letter of credit, program (**LC**) letter of credit, **DLC DOCUMENTARY LETTER OF CREDIT**: we sell (**DLC**) documentary letter of credit, sell (**DLC**) documentary letter of credit, monetize (**DLC**) documentary letter of credit, asset monetization (**DLC**) documentary letter of credit, duplicate (**DLC**) documentary letter of credit, asset duplication (**DLC**) documentary letter of credit, bullet (**DLC**) documentary letter of credit, program (**DLC**) documentary letter of credit, **BG BANK GUARANTEE**: we sell (**BG**) bank guarantee, sell (**BG**) bank guarantee, monetize (**BG**) bank guarantee, asset monetization (**BG**) bank guarantee, duplicate (**BG**) bank guarantee, asset duplication (**BG**) bank guarantee, bullet (**BG**) bank guarantee, program (**BG**) bank guarantee, **MTN MEDIUM TERM NOTE**: monetize (**MTN**) medium term note, asset monetization (**MTN**) medium term note, duplicate (**MTN**) medium term note, asset duplication (**MTN**) medium term note, bullet (**MTN**) medium term note, program (**MTN**) medium term note, **BD BANK DRAFT**: monetize (**BD**) bank draft, asset monetization (**BD**) bank draft, duplicate (**BD**) bank draft, asset duplication (**BD**) bank draft, bullet (**BD**) bank draft, program (**BD**) bank draft, **BS BANK STATEMENT**: duplicate (**BS**) bank statement, asset duplication (**BS**) bank statement, bullet (**BS**) bank statement, program (**BS**) bank statement, **SKR SAFEKEEPING RECEIPT**: monetize (**SKR**) safekeeping receipt, asset monetization (**SKR**) safekeeping receipt, duplicate (**SKR**) safekeeping receipt, asset duplication (**SKR**) safekeeping receipt, bullet (**SKR**) safekeeping receipt, program (**SKR**) safekeeping receipt, **GB GOLD BANK**: monetize (**GB**) gold bank, asset monetization (**GB**) gold bank, duplicate (**GB**) gold bank, asset duplication (**GB**) gold bank, bullet (**GB**) gold bank, program (**GB**) gold bank, **DB DIAMONDS**: monetize (**DB**) diamonds, asset monetization (**DB**) diamonds, duplicate (**DB**) diamonds, asset duplication (**DB**) diamonds, bullet (**DB**) diamonds, program (**DB**) diamonds, **LTN NATIONAL TREASURY BONDS EUROCLEAR**: monetize (**LTN**) national treasury bonds Euroclear, asset monetization (**LTN**) national treasury bonds Euroclear, duplicate (**LTN**) national treasury bonds Euroclear, asset duplication (**LTN**) national treasury bonds Euroclear, bullet (**LTN**) national treasury bonds Euroclear, program (**LTN**) national treasury bonds Euroclear, **GBW GLOBAL BONUS**: monetize (**GBW**) global bonus, asset monetization (**GBW**) global bonus, duplicate (**GBW**) global bonus, asset duplication (**GBW**) global bonus, bullet (**GBW**) global bonus, program (**GBW**) global bonus, **SG SOVEREIGN GUARANTEE**: monetize (**SG**) sovereign guarantee, asset monetization (**SG**) sovereign guarantee, bullet (**SG**) sovereign guarantee, program (**SG**) sovereign guarantee, **PRE SWIFT MT 799**: monetize **PRE-SWIFT MT 799**, asset monetization **PRE-SWIFT MT 799**, bullet **PRE-SWIFT MT 799**, **PRE-SWIFT MT 799** program, **SWIFT MT 760**: **SWIFT MT 760** monetization's, **SWIFT MT 760** bullet, **SWIFT MT 760** program, **OTHER**: group, **JOSE ANTONIO IGLESIAS BANUELOS, INTERNATIONAL PURCHASE OF ASSET S.L. B44510014, INTERNATIONAL ASSET OPERATIONS S.L.U. B12710067, SWITZERLAND, AUSTRALIA, SPAIN, LONDON, HONG KONG, GERMANY - WWW.BANK-TO-BANK.ES - JULY 22, 2026.**

