FIREFISH ESCROW POLICY
Effective as of: 26/November/2026

Capitalized terms used in this document shall, unless otherwise defined herein, have the meanings ascribed to them in the Terms of Service for the Firefish platform.

Firefish Europe s.r.o. („Firefish“ or „we“) provides the Escrow setup support and Bitcoin collateral escrow services in accordance with the rules, terms and conditions as prescribed in the applicable documentation, most notably Terms and Applicable escrow rules, as well as with other policies or procedures as they are or may, from time to time, be published on, or otherwise be accessible from, the Site (all such rules, terms and conditions hereinafter referred to as the „Escrow Policy“).

The following text contains a non-exhausting summary of the Escrow Policy, mainly from technical and security aspects highlighted below and is designated to users transferring their Bitcoin collateral into the environment used for the Bitcoin collateral escrow („client“):

1. ESCROW ARCHITECTURE AND CONTROL OVER CRYPTO-ASSETS

Firefish implements the escrow of Bitcoin (BTC) through a two-layer Escrow environment, consisting of:

- **Prefund Address** – a technical address used to prepare the collateral;
- **Escrow Address** – a 3-of-3 multisignature address used to hold the collateral during the term of financing.

Firefish does not provide traditional custodial storage of crypto-assets on centralized wallets. Instead, limited control over the collateral is exercised through the possession of private keys necessary for the execution of partially pre-signed Bitcoin transactions, while signatures are added only upon fulfillment of specific pre-defined contractual conditions.

2. DISTRIBUTION OF PRIVATE KEYS AND SIGNING LOGIC

The Escrow Address is managed under a 3-of-3 multisignature scheme, with keys distributed as follows:

- **Price Oracle Key** – held by Firefish,
- **Payment Oracle Key** – held by Firefish,
- **B – EPH Key** – generated and solely held by the Firefish Borrow user.

The B – EPH key is intentionally discarded by the Firefish Borrow user after signing the required transactions, reducing the risk of unauthorized access.

3. PROTECTION AGAINST UNAUTHORIZED DISPOSITION

All transactions related to the Escrow Address (*Tx_repayment*, *Tx_default*, *Tx_liquidation* and *Tx_recover*) are pre-created and partially (in case of *Tx_recover* even fully) signed, while having pre-determined outputs (destination addresses). Following the creation and partial signature of these transactions and after the B-EPH key has been discarded, it is not possible to effectively sign any other transaction with regards to the Escrow Address. Firefish cannot access or dispose of BTC in any other way than by adding the missing signature or signatures (in our roles as Oracles) to the already existing transactions.

4. FALLBACK AND COLLATERAL RECOVERY

The Escrow environment includes a *Tx_recover* transaction that is pre-signed by all three required keys and is time-locked (i) in case of a Marketplace loan, until one month after the end of the financing period, and (ii) in case of an Instant loan, until four years and two months after the Loan provision date (as defined in the respective Loan and security agreement) of the loan in connection with which the respective Escrow environment was established. The timelock of each *Tx_recover* transaction is set upon its creation and pre-signing in accordance with the Escrow Policy as in effect at that time and cannot be altered once the transaction has been signed. This transaction allows recovering the collateral if no standard settlement takes place.

5. SEGREGATION OF ASSETS

Each Escrow environment is tied to a concrete financing agreement and established individually. There is no commingling of different client's assets, or between clients and Firefish.

6. PROTECTION AGAINST FRAUD AND CYBERSECURITY THREATS

Client communication with Firefish takes place using TLS encryption via the Firefish App, access to which requires client login with password and allows setting up two-factor authentication (2FA).

We do not obtain or store clients' private key (B-EPH Key).

Oracle signatures are provided only under clearly defined conditions in the documentation (Applicable escrow rules).

The system architecture avoids any single point of failure – no single party can control client assets unilaterally (in a discretionary manner).

All Bitcoin transactions are conducted on-chain (Bitcoin Blockchain), ensuring auditability and immutability.

7. REGISTER OF POSITIONS

Firefish satisfies its legal obligation to maintain a register of positions through a dual-layered approach:

- **Bitcoin Blockchain** – All crypto-assets (BTC) held as collateral in connection with the Firefish Borrow service are deposited into uniquely generated 3-of-3 multisignature Escrow addresses. These addresses are linked to individual client financing arrangements. All movements of crypto-assets (BTC) (e.g. funding, returning, liquidation) are recorded as on-chain Bitcoin transactions, serving as an immutable and transparent technical position register.

- **Internal Records** – In parallel, we maintain an internal system mapping all Escrow addresses and transactions to specific Users. This system reflects the client's entitlements to crypto-assets and tracks the status of each financing lifecycle (e.g. active loans, overdue, liquidated).

Whenever requested by the client, and in cases where the Collateral escrow lasts for at least three months, Firefish shall, in accordance with Article 75(3) of the MiCA Regulation, provide a statement of the crypto-asset position recorded in the name of that client. This position

statement shall be issued in electronic format and identify the relevant crypto-assets, their balance, their value, and any transfers of crypto-assets made during the relevant period.

8. LIABILITY FOR THE LOSS OF CRYPTO-ASSETS

Firefish shall be liable to its clients for the loss of any crypto-assets (BTC) or of the means of access to such crypto-assets as a result of an incident that is attributable to Firefish. Our liability shall be limited to the market value of the crypto-asset that was lost at the time the loss occurred.

Incidents not attributable to Firefish include any event in respect of which we demonstrate that it occurred independently of the provision of the relevant service or independently of the operations of Firefish, such as a problem inherent in the operation of the distributed ledger (Bitcoin Blockchain) which Firefish does not control.