Bank Frick AG
Landstrasse 14
9496 Balzers
Liechtenstein

T +423 388 21 21
F +423 388 21 22
bank@bankfrick.li
www.bankfrick.li

ID no.
FL-0001.548.501-4
VAT no. 53884

# Bank Frick AG Custody Policy

Version 1.0 of 1 February 2025

This Custody Policy describes the principles for the secure, legally compliant custody of cryptoassets and corresponding private keys in accordance with the regulatory requirements of the Regulation (EU) 2023/1114 on markets in cryptoassets (MiCAR), the Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA), as well as the supervisory rules and regulations of Liechtenstein.

## Summary of services provided

As part of its business activities, Bank Frick AG («Bank Frick») offers a custody service for cryptoassets and corresponding private keys. The Bank's objective is to hold its clients' cryptoassets in secure custody, while affording these clients easy access to their tokens.

## Regulatory requirements

The client acknowledges that international, European and/or Liechtenstein legal regulations on anti-money laundering, and the combating of organised crime and financing of terrorism (including legal regulations concerning due diligence) mean that the Bank is duty bound, both prior to and during the period of custody, to examine the tokens to be held in custody particularly with regard to their origin, source and authenticity and for the existence of any possible blocking flags, and that the Bank may conduct forensic examinations and any other investigations it deems necessary. All transactions are subject to applicable anti-money laundering laws.

## Technical and process-related aspects of custody

Bank Frick accords the highest priority to the security of the cryptoassets held in its custody. Bank Frick deploys diverse technologies to ensure the secure custody of the cryptoassets. Bank Frick's custody solution is certified according to CCSS Level III, SOC2 Type II and ISO 27001.

### Custody technology

Multi-Party Computation (MPC): technology for generating, storing and using cryptographic signature keys for protecting cryptoassets and cryptographic instruments. Keys generated and used within the MPC system are never stored in the same location. Each key is instead generated in such a way that the result is shared between two or more parties without any one party able to see more than their own specific part, which in itself is meaningless. Alongside this, the signature is created without the individual parts ever becoming merged together. This prevents the situation where hackers who gain access to a subset of computers from then extracting important material. Since all MPC parties must review the transaction according to the guidelines, this also makes it impossible to bypass the security measures installed to prevent the misuse of keys.

## Custody model

Bank Frick only holds certain select cryptoassets in its custody, and it generally uses the Omnibus model for this purpose. With the Omnibus model, the cryptoassets of a number of clients are stored on shared distributed ledger (DLT) addresses and retained in wallets controlled by Bank Frick. From an operational perspective, the unique assignment of cryptoassets to the relevant clients is performed via an internal accounts system and the process is permanently trackable. This unique assignment process means the cryptoassets are separable if ever Bank Frick were to become insolvent.

## Access to cryptoassets

Bank Frick offers a range of (technical) access channels to its custody solution:

- Cryptoassets are deposited and withdrawn through client advisers
- Cryptoassets are traded through the client advisers, the trading desk, or via the user front-end (online banking). In selected cases, trading is also performed via Application Programming Interfaces (APIs).

The custody solution itself is directly linked to various distributed ledgers (or «blockchains»). As a rule, clients' cryptoassets are transferred into the custody of Bank Frick to the addresses controlled by the Bank via the relevant client address blockchains. Outbound transactions are initiated by client advisers, and executed via the relevant blockchain.

## Wallet structure

Bank Frick offers the following wallet classes: hot, warm and cold wallets. This wallet structure aims to provide the greatest level of security combined with high accessibility to the cryptoassets.

- Hot wallets: Hot wallets are permanently connected to the internet and allow for fast, easy access to the cryptoassets held in custody. Hot wallets are particularly used in the execution of frequent, small-scale transactions.
- Warm wallets: To make outbound transactions from warm wallets, it is first necessary to have a manual interaction (transaction release) with Bank Frick employees. Warm wallets are used to make ad hoc, medium-sized transactions. Bank Frick holds a large share of client cryptoassets in warm wallets.
- Cold wallets: Cold wallets are not connected to the internet. To make outbound transactions from cold wallets, it is essential for a manual interaction (transaction release) to take place; this interaction is larger in scope compared to the transaction release applied with warm wallet transactions. Cold wallets are used to perform infrequent and very large-sized transactions. The main share of Bank Frick's client cryptoassets are held in cold wallets.

## Contingency and recovery plans

To ensure that cryptoassets remain continuously available, Bank Frick operates a wide-ranging Business Continuity Management (BCM) system, which includes strategies for maintaining the continuity of operations during crisis situations. Contingency and recovery plans designed for wallets and digital assets ensure that even unforeseen outages have no long-lasting negative effects. Targeted cybersecurity and incident response measures make it possible to respond to potential security threats.

### Control procedures and processes

Bank Frick has implemented a range of control procedures and processes to ensure the security of clients' cryptoassets held in the Bank's custody. Notable measures include:

- Bank Frick fulfils the ISO-Norm 27001 standard on cyber resilience alongside all the requirements of Regulation (EU) 2022/2554 (DORA) on ensuring digital operational resilience.
- Private key management (only in combination with cryptoassets): Bank Frick applies the greatest diligence and caution in administering the private keys needed to access clients' cryptoassets. These private keys are retained in a secure location, which is both physically and digitally protected. These private keys are never provided nor disclosed to any third party. They may only be used by authorised persons. The storage of private keys and the transaction signature procedure are implemented using technologies such as Multi-Party Computation («MPC»).
- Transaction release: Bank Frick applies a strictly defined procedure for approving outbound warm and cold wallet cryptoasset transactions. Employees who perform transactions from warm or cold wallets are subject to strict identity and access controls. A multi-factor authentication process - which includes the entry of PINs, passwords, codes and biometric data - must be completed before transactions can be executed. During this process, all transactions are reviewed and/or approved by a number of persons holding various roles and responsibilities. Prior to execution, the transactions are assessed based on a range of criteria, including the amount, frequency, recipient and risk.
- Employees are given regular training to enhance their awareness of current security issues.
- Regular external and internal audits ensure that the systems and processes of Bank Frick are continuously assessed in terms of security. This means they can be modified whenever necessary.

## Legal aspects of custody

### Separation of cryptoassets

The cryptoassets held in the Bank's custody remain in the ownership of the respective clients, and they are managed as legal property separate from Bank Frick's own cryptoassets, especially in the event of any insolvency or enforcement proceedings.

### General Terms and Conditions

The Bank holds its clients' cryptoassets in custody in accordance with its General Terms and Conditions, including its custody rules, which are available to view on the Bank's website. These terms, conditions and rules form an integral part of this Custody Policy.