Flowdesk™

Flowdesk
231 Rue Saint-Honoré
75001 PARIS

Custody Policy

Version	Number	1
	Date of creation	01/03/2023
Written by	Anne-Sophie Cissey Head of Legal and Compliance	
Validated	By	Paul BUGNOT
	Date	16 March 2023

This Policy shall apply to all the companies that form part of the Flowdesk Group (referred as "FLOWDESK") which is composed by:

- Flowdesk, Société par Actions Simplifiées formed on 01 April 2020, registered in the Paris Trade and Companies Register under number 883604647 and whose registered office is located at 231 rue de Saint Honoré, 75001 Paris. Flowdesk is registered with the AMF under the number E2021-19 as a DASP (Custody, selling and buying digital assets)
- Flowdesk Asia Pte Ltd., formed on 22 February 2022, registered in the Singapore Trade and Companies Register under number 202206308E and whose registered office is located at DOWNTOWN GALLERY, 6A SHENTON WAY, #04-01, 068815.
- Flowdesk US Inc. formed on 12 December 2022, registered in the Delaware Trade and Companies Register and whose registered office is located at 8 the Green Ste R, in the City of Dover County of Kent 19901.

This Policy has been prepared to comply with our disclosure obligations under DDADUE adopted on the 28th of February in relation to safekeeping of digital assets.

This Policy is not intended to be, and should not be relied upon as, legal, financial, tax, accounting or other advice. Unless otherwise expressly agreed in writing, FLOWDESK is not providing anyone with any such legal, financial, tax, accounting or other advice.

This Policy refers to Flowdesk's Custody offer. This policy sets out how the requirements are complied with in practice in terms of roles and responsibilities. It does not provide details of the substantive requirements.

I. General requirements

FLOWDESK is a regulated custodian under the laws of France. The Group provides its clients with solutions to maintain, secure and monitor the client's private keys allowing access to their digital assets wallet.
This activity is regulated in France by the "Loi Pacte" voted in 2019, Articles L. 54-10-1 to L. 54-10-5, D. 54-10-1, D. 54-10-2, D. 54-10-7 and D. 54-10-9, L. 561- 1 et seq. and R. 561-1 et seq. of the Monetary and Financial Code as well as Articles 721-1-1, 721-3 to 721-6 and 722-1, 722-4, 722-5, 722-7, 722-13 and 722-14 of the AMF General Regulation.
Custody is defined by the Article D. 54-10-1 1° of the Monetary and Financial Code as "the act of controlling, on behalf of third parties, the means of access to the digital assets registered in the DLT and of keeping a register of positions, opened in the name of the third party, corresponding to the third party's rights to said digital assets"[1].

[1] DOC2020 07 Questions answers relating to the digital asset service providers regime

This applies only when FLOWDESK ensures the custody of the private keys and excludes when FLOWDESK deals with the client's assets through API keys.

FLOWDESK undertakes to set up all the procedures and means to render the funds under its custody to its clients and commits to the AMF's requirements:

- Segregation
- Security
- AML-FT procedures (please refer to Appendix 1)
- Risk disclosure (please refer to Appendix 2)

a- Segregation and Transparency

FLOWDESK ensures that the digital assets of its clients are segregated from its own assets in different ways:

- Sub-account
- Sub-wallet
- Specific accounting, associating one transaction to one client.

When opening a custody account with FLOWDESK, a sub-wallet with FLOWDESK's subcustodian(s) is opened for the client. The necessary information is mapped on a register designed for this purpose by FLOWDESK.
FLOWDESK might act on the client's assets from time to time subject to the client's instructions. This includes but is not limited to transfer, trading or selling of digital assets. FLOWDESK will require a clear instruction given by any mean by the client (including and not limited to Telegram, Email, Voice). In any case, FLOWDESK will produce an execution report to confirm the transaction showing, when relevant, the transaction ID, the nature of the operation, the involved amount, and the traded assets. The account holder can monitor the service using Looker, a tool specifically designed for this use. It shows all his balances on every subcustodian and can help him monitor and manage the counterparty risks.

When sending the funds to an Exchange or any other third-party in such a way that FLOWDESK does not hold the private keys of the wallet anymore, FLOWDESK's liability shall be limited to the strict management of the account. FLOWDESK shall be held responsible only in case of gross negligence and/or fraud. However, FLOWDESK shall maintain sub-account in the name of each client with this third party every time it is possible. FLOWDESK is not authorized to commingle the assets of its clients and shall ensure a strict accounting of the assets of each client.

The Client shall always remain in capacity to manage its assets and its exposure to third party by knowing what counterparty is involved and in which proportion. If the Client decides to transfer back part or all its assets on one or multiple wallet(s), FLOWDESK shall execute his demand without any delay.

b- Security

FLOWDESK shall maintain the highest security standards. Therefore, FLOWDESK has developed a robust operational risk and resilience framework to ensure the availability and safe custody of the assets.

FLOWDESK has adopted a risk framework to monitor and manage the risk. This work is organized around 4 big steps:

- Risk Identification
- Risk Assessment
- Risk Mitigation
- Risk Monitoring

In the course of this work, FLOWDESK has envisioned several main threats:

- Human failure (or Fraud)
- Cybersecurity
- Third-Party failure

Human Failure has been limited through a systematic supervisory. Each significant operation must be ensured by at least 2 persons (four eyes rule). This control is being doubled by a throughout check by FLOWDESK's Internal Control team. Moreover, FLOWDESK's teams are submitted to regular trainings including risk management. FLOWDESK profits from a 24/7 coverage of technical support both on the Technological, Compliance, Trading and Financial issues.

Cybersecurity is a major challenge for FLOWDESK. A cybersecurity policy has been adopted by FLOWDESK. The Company complies with DORA Regulation[2] and has put in place an ICT (information and communication technology) risk management which includes an Incident Log provided to all staff. FLOWDESK has also tested its digital operational resilience. Each contract, agreement or terms and conditions signed with any ICT provider has been reviewed by the Legal team to ensure that the regulatory standards were enforced. FLOWDESK has defined a business continuity plan including cyber incidents and has trust in its faculty to remain resilient so as to maintain the security of the assets under its custody or to maintain a satisfying level of security while rendering the assets to their owner's wallets. FLOWDESK complies with SOC2 regulation.

FLOWDESK only works with trustable sub-custodian. To nominate a new custodian, it shall comply with SOC2 and ISO 27001 standards. As of today, FLOWDESK works with Fireblocks and Ledger Vault's solutions. If FLOWDESK wants to add another sub-custodian to its offer, it shall submit the name and the main information regarding the security standards ensured by the provider to the client which remains free, always, to refuse that their assets be exposed to this provider. This does not include Exchanges and Third-party providers which rarely comply with Cybersecurity requirements.

[2] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)

II. Sub-custodian

Under this policy, Sub-custodian only refers to the technical solutions selected by FLOWDESK to store its client's assets. It does not include Exchanges and other Third Party Provider. Thereupon, FLOWDESK relies on the following custody solutions:

FIREBLOCKS	Founded in	ISRAEL
	Cryptographic technic	MPC-CMP
	Compliance with	X SOC2 X ISO 27001
	Integrates	X Chainalysis X Nota Bene
	Website	https://www.fireblocks.com/
LEDGER	Founded in	FRANCE
	Cryptographic technic	
	Compliance with	
	Integrates	
	Website	https://enterprise.ledger.com/

FLOWDESK may select a new Sub-custodian from time to time. The Company will give priority to the quality of the services and the security of its clients' assets. These Sub-custodians are selected according to a rigorous process which is part of a detailed procedure enabling Flowdesk to comply with its obligations, in particular under the loi PACTE, and an appropriate policy with regard to its size, its organization and the nature of its activities, with a view to taking reasonable measures aimed at preventing conflicts of interest that could arise from the relationships with these third-party entities. The final selection of a Sub-custodian is approved by a specific committee meeting whenever relevant, headed by a member of the FLOWDESK Executive Committee and with the participation of the manager in charge of the relationships with these third-party entities, the managers of the operational departments concerned and FLOWDESK' Compliance and Legal departments. A contract is signed between FLOWDESK and each of its Sub-custodians, particularly taking into account the aspects relating to the protection of assets. This committee supervises the monitoring and the relationships with the network of these third-party entities, which are managed by the trading team on a day-to-day basis. Throughout the relationship with each sub-custodian, this dedicated and experienced team carries out due diligence checks in order to verify the quality of their services rendered in operational as well as risk management terms as well as with regard to protection of assets and compliance with regulatory and contractual commitments.

As described by the Article 722-2 of the AMF General Regulation, “the responsibility of the custodian of the digital assets towards its client is not affected by the fact that it uses a sub-custodian”. FLOWDESK remains fully liable for the Sub-Custodian. However, FLOWDESK’s liability is limited in the cases where the client asks FLOWDESK to move its funds towards an exchange (CEX or DEX) even if the assets are transferred on FLOWDESK’s accounts. Indeed, in those cases, FLOWDESK shall remain only liable for gross negligence and fraud attributable to FLOWDESK. This complies with Article 722-1, 6° of the AMF General Regulation which provides that “except in the case of events that are not attributable, directly or indirectly, to the digital asset service provider, it shall return control of the means of access to the digital assets to the clients without any delay.
In the event that control of means of access cannot be returned, the digital asset custodian shall compensate its client. Events that are not attributable to the digital assets custodian include any event that the custodian is able to demonstrate is beyond its operational control, including an inherent problem with the distributed ledger system or a smart contract that may be based on a distributed ledger system which is beyond its control.” FLOWDESK’s contract and terms and conditions are designed specifically for this purpose.

III. Internal Controls

FLOWDESK’s Custody will be submitted to internal controls led by Flowdesk’s Finance team. It focuses on two steps:

- A governance process involving several layers of security
- Several surprise controls (up to 4) led by Flowdesk’s Finance team per year.
- A complete external audit every 2 years

FLOWDESK’s internal process states that the movement of client’s assets under custody shall involve at least 2 directors of Flowdesk. The Company has adopted the principle of the Segregation of Duties. The communication with the client regarding their assets under Custody shall remain the Middle Office’s responsibility. The Finance Team will be in charge of controlling the work of the Middle Office regularly. To ensure independence and reliability of the audits, an external audit will be led every 2 years.

During internal controls, the auditor will check that the assets held in Custody with the Sub-custodian match the reports’ balance and Looker’s display. The auditor will check the history of the operations executed by and/or for the clients and will analyze if this historic matches with the filed documentation for each client.

The auditor who performs the examination will issue an opinion noting whether the adviser was in compliance with the regulations regarding the segregation of the funds and the trustworthiness of the documentation and reports provided by FLOWDESK.

The audited documentation shall include:

- A complete review of client’s contracts to identify which accounts are subject to custody

- Legal opinion for complex situations where it's not immediately clear whether custody has been triggered
- An updated account listing which identifies those accounts that are subject to examination
- A contracts with clients and custodians, including the latest amendments, if any
- Current contact information (addresses, phone numbers, email addresses) for clients, custodians, and counterparties
- Internal control documentation explaining how systems and processes work - in particular, these should address trading, reconciliation, process for evaluating custody concerns, and other key areas
- Organized records supporting all transactions
- Position and transaction reconciliations

If the auditor finds any material discrepancies during the surprise examination, the auditor must notify the client of such findings within one business day.

If the auditor resigns or is dismissed from the surprise examination engagement, the auditor must file a statement notifying the Supervisory Board of date and reasons (such as problems relating to the examination) for the resignation or dismissal within four business days.

IV. Record Keeping

FLOWDESK maintains records of digital assets held in custody. In particular, FLOWDESK will:

- register in its record all the shared information, including the notional amount of such assets; and
- be able to provide, at any time, a comprehensive and up-to-date inventory of the Client's assets, including their notional amounts

FLOWDESK must ensure that records reflect any changes in ownership of such assets. FLOWDESK's ability to carry out its record keeping obligations is dependent on:
- having knowledge of such events; and
- receiving appropriate documentation and/or information from the Client or third parties, which constitutes evidence of ownership

Therefore, FLOWDESK is required to put in place procedures to ensure that it is informed of any assignment, transfer, exchange or delivery of the client's assets. In general, the measures required by FLOWDESK are ex-post procedures, rather than ex-ante controls.

FLOWDESK may either keep its own record of "other assets" which it is satisfied that the Client owns or it may choose to rely on the records kept by the Sub-custodian.
If FLOWDESK wishes to delegate its record keeping obligations to a third party, it should check whether there is any local regulation or legislation which may prohibit it from delegating its record keeping obligations to a particular entity.

Even where there is no prohibition on delegation, FLOWDESK should ensure that it identifies and manages any risks appropriately; including any conflicts of interest or procedural deficiencies which mean there that the records may not be fully up to date.
FLOWDESK should also ensure that it complies with any applicable outsourcing requirements when delegating record keeping obligations.

FLOWDESK is required to set up and maintain an escalation procedure for situations where an anomaly in ownership details is detected including notification to the Client and to the competent authorities eventually if the situation cannot be clarified.

V. Default of Flowdesk

In this document, "Default" shall mean any event or situation that jeopardizes the fulfillment of a custodian or sub custodian mission, that is to say, to render the funds in a timely manner.

The client shall remain the sole owner of the assets under Custody at all times. As required by the Article 722-1, 6° of the AMF General Regulation FLOWDESK "shall ensure that the necessary procedures are in place to return the means of access to the digital assets [...]". This means that the client's assets can't be used to pay back FLOWDESK's creditors. FLOWDESK's documentation like ownership records and custody agreements shall be used to demonstrate the ownership of the assets.

The following procedure shall be observed in three crisis situations:

- Any case of material and/or technical risk of such nature that the assets under Custody are jeopardized
- A solvability risk
- A liquidity risk

When one of those risk occurs, FLOWDESK shall appoint one of his representatives as Crisis Manager. For the purpose of this policy, this Crisis Manager shall be appointed by the Risk Management Committee gathered within a maximum of 3 business days.

The Crisis Manager shall establish the balance of the client's assets and their location (hot/cold wallet, on/off Exchanges) at the beginning of the crisis. The Crisis Manager shall produce a report including the methodology used to identify the balance of each client and the results of his inquiry. The scope of this audit shall be limited to assets under Custody on Flowdesk's wallets (that is to say a wallet whose private key is fully controlled by FLOWDESK and/or account on Exchanges opened under FLOWDESK's name). The results of the audit shall be presented to the Head of Finance. If approved, the Crisis Manager shall pursue the operation.

The second step focuses on recentralizing the assets on wallets controlled by FLOWDESK. The Crisis Manager will be in charge of operating the transactions and validating the operations with Exchanges. FLOWDESK will need to prepare and maintain a register of transactions under this special procedure. At the end of this step, the Finance team shall control the final balances and check their accordance with the results of the previous analysis. At the end of this process, the client shall be notified by email of the current operation.

In case of any discrepancy during those controls, FLOWDESK shall contact the regulator and inform the clients within 48h.
Five business days after the notification, the Crisis Manager shall render the funds to the Clients' whitelisted wallets. The transactions shall be registered in a special document made available to independent auditors and litigators.

VI. Default of a third party

The default of a third party (an Exchange or another partner) only presents a risk for the client in the case where FLOWDESK keeps the assets of its clients on its own accounts opened in its name.

First, the Client shall remain always in the capacity of exposing itself to a counterparty or to withdraw from it. The decision shall be always documented by FLOWDESK, and the tools made available to the clients to monitor their exposure shall remain truthful. FLOWDESK cannot be held liable of a third party's liquidation. Since the client remains in control of his funds and since the default of a third party cannot be attributable to FLOWDESK, no compensation or refund can be claimed by the client.

FLOWDESK is not allowed to transfer any fund to any counterparty not duly authorized by the client. If this situation should occur, the client would be entitled to a full refund by FLOWDESK. If FLOWDESK or any of his representatives and/or employees is guilty of fraud or gross negligence, the client would also be entitled to a full refund.

The present policy might be reviewed from time to time by the Executive Committee of the Company

Appendix 1: AML-FT Procedure Executive Summary
Appendix 2: Risk Disclosure