Market Abuse Policy

Creation Date		March 30th, 2021
Version	**N°:**	4
	Validated by:	Anne-Sophie CISSEY
	On:	March 5h, 2023
Updated on:		March 5h, 2023
Distribution list		Flowdesk’s staff

FOREWORD

Best practices and recommendations from financial authorities regarding crypto asset trading have led Flowdesk to adopt administrative and organisational rules and processes to prevent market abuse.

This Market Abuse Policy, as defined by the MAR Regulation, EU 596/2014 aims to ensure that all employees comply with insider trading rules and do not misuse, or place themselves under suspicion of misuse, of inside information they may be deemed to hold, including in the periods leading up to an announcement on crypto assets and their issuers.

This policy is intended to promote compliance with the relevant obligations and restrictions under the regulations on traditional markets, including the Market Abuse Regulation. Nothing in this policy sanctions a breach of the Market Abuse Regulation, the insider trading provisions of the Economic Crime Act or any other relevant legal or regulatory requirement.

This policy applies to all employees (including salaried employees, freelancers, interns and trainees). As this policy indicates, there are parts that apply only to certain employees of the company.

DEFINITION OF MARKET ABUSE

Market abuse is defined as:

1. the conclusion of a transaction, the placing of a transaction order or any other behaviour that

    ○ gives, or is likely to give, false or misleading signals as to the supply, demand or price of Flowdesk customers' crypto assets

    ○ or secures, or is likely to secure, the price of one or more crypto-assets unless the person entering into a transaction placing a trade order or engaging in any other conduct establishes that such transaction, order or conduct was entered into for legitimate reasons and is consistent with accepted market practice

2. entering into a trade, placing a trade order or any other activity or behaviour that affects or is likely to affect the price of one or more of Flowdesk's clients' crypto-assets

3. the dissemination of information through the media, including the internet, or by any other means, which gives, or is likely to give, false or misleading signals as to the supply, demand or price of a client's crypto asset, or is likely to set the price of one or more client-issued crypto assets at an abnormal or artificial level, including the dissemination of rumours, where the person making the dissemination knew, or ought to have known, that the information was false or misleading

4. the transmission of false or misleading information or the provision of false or misleading material in relation to a reference asset, where the person who made the transmission or provided the material knew or ought to have known that it was false or misleading.

COMPLIANCE DEPARTMENT

The Compliance Department has the duties and powers set out in this policy. The Management Team may assign additional duties or powers to the Compliance Department. The Compliance Department may, in exceptional circumstances and in consultation with the Senior Management Team, grant exemptions from the prohibitions, restrictions or obligations set out in this Policy.

IDENTIFIED RISKS OF MARKET ABUSE

Prohibition of insider trading

Employees who have inside information are prohibited from trading in the crypto-assets to which the inside information relates. In addition, an employee is prohibited from trading during any period in which the compliance department has prohibited the employee from doing so.

This prohibition does not apply if the employee makes a transaction in fulfilment of an obligation that has become due in good faith and not for the purpose of circumventing the insider trading prohibition or for any other illegitimate reason and :

1. this obligation arises from a previous order or agreement;

2. (or) the transaction is made to satisfy a legal or regulatory obligation that arose before the employee concerned was made aware of inside information.

Where the employee is a legal person, the trading restrictions shall also apply, in accordance with national law, to natural persons who participate in the decision to acquire, dispose of, cancel or modify an order on behalf of the legal person concerned.

Prohibition of disclosure

Employees are prohibited from illegally disclosing privileged information to a third party, unless the disclosure is made in the normal course of employment, profession or duties.

Employees with inside information are prohibited from recommending or inducing another person to trade in the crypto assets of Flowdesk customers.

Market manipulation

Employees are prohibited from engaging or attempting to engage in market manipulation.

Employees are required to provide all assistance reasonably required for the purposes of an investigation by the Compliance Department.

If an Employee is in doubt as to whether a prohibition under this Policy or applicable law applies, he or she may seek advice from the Compliance Department. However, Employees remain responsible for compliance with this Policy and applicable law and should obtain their own legal advice if necessary or appropriate.

If an Employee is in doubt as to whether a prohibition under this Policy or applicable law applies, he or she may seek advice from the Compliance Department, it being understood that any guidance or advice provided by the Compliance Department is advisory only. However, Employees remain responsible for compliance with this Policy and applicable law and should obtain their own legal advice if necessary or appropriate. Ultimately, it is the Employee's responsibility to decide whether to trade in Flowdesk securities. Regardless of the guidance or advice of the Compliance Department, if the Employee fails to comply with his or her legal obligations, he or she may be subject to sanctions.

The compliance officer can be contacted by e-mail at the following address: **compliance@flowdesk.co**

ADDITIONAL RULES FOR SENSITIVE EMPLOYEES

Prohibited periods

A sensitive employee is prohibited from trading in client crypto-assets during blackout periods, whether or not he/she possesses inside information, unless he/she obtains permission from Flowdesk.

Outside the blackout periods, a sensitive employee is allowed to trade, unless he or she has inside information.

A sensitive employee must report to the compliance officer each transaction in customer crypto-assets made on his or her own behalf on the third business day following the date of that transaction.

Long-term investments

If a sensitive employee holds client-issued crypto-assets, they must hold them for long-term investment purposes. Employees are prohibited from buying or selling options on client-issued crypto-assets or short selling client-issued crypto-assets.

Declarations

A sensitive employee must report to the compliance department each transaction involving crypto-assets issued by a customer

The Compliance Officer must have received the request by 13:00 (CET) one working day before the intended trade date (or other event triggering the notification requirement). The request must be accompanied by a draft containing full details (to the extent available). On the date of the transaction (or other notification event), the sensitive employee must confirm (or amend) these details. The Compliance Officer may make additional requirements.

The prohibitions defined by this policy remain applicable to the sensitive employee for a period of three months after the end of his/her duties.

A sensitive employee (other than the president of Flowdesk) or a compliance officer must not trade in client issued tokens without first informing the president and must receive permission to trade from the president.

Managing directors must not trade in client-issued tokens without first informing the president of Flowdesk and receiving permission to trade from him or, if the president of Flowdesk is not present, without first informing the compliance department and receiving permission to trade from that person.

A response to a request for transaction authorisation should normally be given within two working days of the request.

Flowdesk will keep a record of the response to any transaction request made and any authorisation given. A copy of the response and authorisation (if any) will be given to the person concerned.

A person who receives authorisation to carry out a transaction must do so as soon as possible and in any event within two working days of receiving the authorisation.

TRANSACTIONS PERMITTED DURING BLACKOUT PERIODS

Authorised transactions

In the following circumstances, trading by a restricted person who is not in possession of inside information may be permitted during a blackout period:

1. on a case-by-case basis due to the existence of exceptional circumstances, such as severe financial difficulties, which require the immediate sale of crypto-assets issued by customers;

2. or because of the characteristics of the relevant transaction for transactions in which the interest in the relevant crypto-asset does not change, provided that the sensitive employee can demonstrate that the particular transaction cannot be executed at any other time than during the blackout period.

Permission may be given to an individual to sell (but not buy) client-issued crypto-assets when this policy would otherwise prohibit the individual from doing so. Only the designated Compliance Officer can determine whether the individual in question is in serious financial difficulty or whether other exceptional circumstances exist.

Exceptional circumstances

A sensitive employee must provide a reasoned written request to the compliance department to obtain Flowdesk's permission to proceed with the immediate sale of customer-issued crypto-assets during a blackout period. The written request must describe the intended transaction and explain why the sale of crypto-assets is the only reasonable alternative to obtain the necessary funding. When considering whether the circumstances described in the above-mentioned written request are exceptional, the Compliance Officer shall be guided by the indicators set out in the Market Abuse Regulation and related guidelines and standards.

Circumstances are considered exceptional when they are extremely urgent, unforeseen and compelling and when their cause is external to the sensitive employee and the sensitive employee has no control over them. Flowdesk takes into account, among other indicators, whether and to what extent the sensitive employee :

1. has a financial commitment or legally enforceable claim at the time of application

2. has to pay or is in a situation entered into prior to the commencement of the restricted period requiring payment of an amount to a third party, including a tax obligation, and cannot reasonably satisfy a financial obligation or claim by any means other than the immediate sale of the customer issued crypto assets

REPORTING

Reporting obligations of sensitive persons

Each sensitive employee must promptly, and no later than three business days from the date of the transaction, notify the compliance department of any transaction in customer crypto-assets made or conducted by him or on his behalf. A non-exhaustive list of transactions that must be notified is included below.

This notification may be delayed by a sensitive employee until such time as transactions on his or her own account amount to at least €5,000 per calendar year.

Sensitive employees will at all times remain ultimately responsible for meeting their notification obligations in a timely manner.

Reportable transactions

The transactions in client-issued crypto-assets that must be notified to the Compliance Officer are as follows:

1. acquisition, disposal, short sale or exchange
2. entering into or exercising swaps involving the crypto-assets issued by clients
3. transactions in derivatives or related to clients' crypto-assets
4. entering into a CFD on a client-issued crypto asset or auction products based on it 5. the acquisition, assignment or exercise of rights, including put and call options, and warrants on crypto-assets issued by clients
6. subscription to a client's ICO
7. transactions conditional on the fulfilment of conditions and the actual execution of the transactions
8. whether or not to automatically convert a crypto asset issued by a client into another crypto asset
9. gifts and donations made or received and inheritances received
10. transactions executed within indices, baskets and derivatives containing one or more tokens issued by a client
11. transactions executed in shares or units of funds containing crypto-assets issued by customers
12. transactions executed by a third party under an individual portfolio or asset management mandate for the account or benefit of a sensitive employee
13. borrowing or lending of customer-issued crypto-assets, derivatives or any other related financial instruments

LIST OF INSIDERS

Taking the recommendations of the MAR Regulation as a model, Flowdesk keeps a list of persons who have access to inside information (the insider list). The list includes the following information:

1. Name (first name, surname, maiden name)
2. The telephone number
3. The name of the company (if freelance), of the school (if trainee)
4. The function and reasons for including the person in the list
5. The date from which the person obtains confidential information
6. The date on which a listed person ceases to have confidential information
7. The date of birth of the person
8. The identity card number
9. The person's home address
10. The date the list was created and the date it was updated

The Insider List is maintained by the Compliance Officer who updates it promptly in the following circumstances:

- when there is a change in the reason for inclusion of a person already on the Insider List,
- when a new person has access to Inside Information and must therefore be added to the insider list
- when a person ceases to have access to Inside Information.

Personal data collected in accordance with this policy will be retained for a period of at least five years after the date of registration in the insider list or modification of the data or for any other period required by applicable law. Flowdesk is responsible for processing the personal data to be included in the list. Personal data will only be processed for the purposes specified in this policy or for other purposes permitted by applicable law. A person on the insider list may request the Compliance Officer to view his or her personal data on the insider list. Upon request, the Compliance Officer will provide the person concerned with a summary of the relevant personal data within four weeks or within the period required by applicable law.

This personal data may be provided to the competent authorities upon request if:

- it is necessary to comply with the applicable legislation
- if it is in the interest of Flowdesk

The information on the insider list will not be provided to other parties, unless required or permitted by law or if a legitimate interest of Flowdesk requires it.

PENALTIES

In the event of a breach of any of the provisions of this policy, Flowdesk reserves the right to impose any sanction it is entitled to impose in accordance with the applicable legislation or the terms of employment applicable to the employee concerned. Such sanctions may include termination of employment by way of dismissal for gross misconduct.

Flowdesk may also inform any authority of its findings.