Anti-Money Laundering/Counter Terrorism Financing/ Anti-Corruption/Whistleblower and Know Your Customer Policy

VERSION	DATE OF VERSION	EDITED BY	DOCUMENT NAME
1.0	05-11-2018	SAM STONE	Swarm AML Policy v1.0 5-11-2018

List of Contents

Audience and Confidentiality

This document is classified as controlled information asset and intended for the internal use of recipients only and may not be distributed externally or reproduced for external distribution in any form without express written permission of the Swarm Foundation (hereinafter Swarm).

Document Properties

Document Title	Anti-Money Laundering/Counter Terrorism Financing/ Anti-Corruption/Whistleblower and Know Your Customer Policy
Version	1.0
Classification	Controlled

Department	Legal and Compliance	Document Owner	Compliance Officer
Creation	Sam Stone	Date	05-11-2018
Verification	Timo Lehes	Date	
Approval	Philipp Pieper	Date	

Spread List

COMPANY	NAME	DISTRIBUTION
Swarm Foundation	Swarm	All Swarm employees, affiliates and contractors

Revision History

Date	AUTHOR	VERSION	DESCRIPTION	CHANGES
04-10-2018	Sam Stone	0.1	Initial Draft	
05-11-2018	Sam Stone	1.0	Update	

List of Abbreviations

AML	Anti-Money Laundering
ML	Money Laundering
CDD	Customer Due Diligence
CO	Compliance Officer
CTF	Counter Terrorism Financing
FATF	Financial Action Task Force
KYC	Know Your Customer
SAR	Suspicious Activity Report
UBO	Ultimate Beneficial Owner
EEA	European Economic Area
EU	European Union
ISA	International Sanctions Act
MB	Management Board
PEP	Politically Exposed Person
VAT	Value-added tax
TF	Terrorist Financing
RBA	Risk Based Approach

Sweeping Clause

Words importing the singular meaning shall include, where the context so admits, the plural meaning and vice versa. Words denoting the masculine gender shall include the feminine and neuter genders and wording denoting natural persons shall include corporations and forms and all such words shall be construed interchangeably in that manner.

PREAMBLE

It is the policy of Swarm Foundation (hereinafter Swarm) to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the financing of terrorist or criminal activities. Swarm will comply with all applicable requirements and regulations in regards to Anti-Money Laundering, Counter Terrorism Financing and Anti-Corruption.

The purpose of our Anti-Money Laundering/Counter Terrorism Financing/Anti-Corruption/ Whistleblower and Know Your Customer Policy (hereinafter AML policy) is to establish the general framework for the fight against money laundering, terrorism financing, corruption and other crimes. Swarm is committed to reviewing the AML strategies and objectives on an ongoing basis and to maintaining an effective AML program to ensure appropriate policies, procedures and internal controls are in place to account for changes in regulations and/or in our business.

Foreseeing a dynamic regulatory environment and the enlarged scope of compliance, the present policy aims to create awareness, safeguard the reputation of Swarm and to protect the company as well as the persons of contract from the risk of being used for activities related to money laundering, for terrorism financing or for the completion of corrupt acts.

Swarm has put policies and procedures in place and in effect with the objective of ensuring that the relevant customer due diligence measures are correctly and completely applied, as well as to specify the professional diligences to be performed by Swarm, its subsidiaries and entities under its control, as well as staff in such entities and relevant staff from third parties, when acting as representatives of Swarm in bases of legal contracts and/or arrangements.

In addition to applicable legal and regulatory obligations which bind Swarm, its investors, its directors and its employees, Swarm has strong ethical values which enforce a culture of compliance in the working environment and in every relation in which Swarm is involved.

SCOPE OF APPLICATION

We are committed to high standards of AML compliance and require management and employees to adhere to these standards in preventing the use of our products and services for money laundering purposes. Adherence to this policy is absolutely fundamental for ensuring that all of our entities, regardless of geographic location, comply with applicable anti-money laundering legislation.

We are committed to adhering to minimum standards of anti-money laundering compliance based on the applicable anti-money laundering laws and regulations and any additional standards from regulatory supervisors which clarify the main statutory duties imposed on our company. In any country/jurisdiction where the requirements of applicable anti-money laundering laws establish a higher standard, our entities located in those jurisdictions must meet those standards.

Our AML program is formulated and directed by the Risk and Compliance Department, but it is the responsibility of all employees to keep ill-gotten funds out of our company.

Definitions

Money Laundering

"Money Laundering" (ML) is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages:

1. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.
2. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.
3. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Predicated Offense

List and examples (non-exhaustive) of crimes, felonies or misdemeanours which local laws consider as source of proceeds which integration to the economy are money laundering:

- Forgery of currency and products
- Violation of the environment legislation
- Murders and grave physical harm
- Kidnapping, unlawful detention and hostage taking
- Trafficking of stolen goods
- Trafficking of migrants
- Forgery
- Extortion
- Smuggling
- Breaches of fiduciary trust, fraudulent bankruptcy and swindling
- Insider trading and market manipulation
- Public and private corruption
- Crimes and offences with criminal conspiracy
- Abduction of minors
- Sexual exploitation of minors
- Pimping
- Drug trafficking
- Offences of terrorism and terrorist financing
- Frauds against financial interests of the State and international institutions
- Violation of legislation on weapons and ammunition
- Tax related crimes as defined by local legislation, when applicable

Terrorism Financing

"Terrorism Financing" (TF) may not involve the proceeds of criminal conduct, but rather an

attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organisations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Act of Corruption

An “Act of Corruption” or a corrupted act makes reference to any action committed by a public or a private person in order to obtain an unfair advantage or illegitimate profit or position by utilising economic means, influence (or access to a person of influence) or force.

The corrupt act does not necessarily need to obtain the unlawful advantage or create unfair conditions.

In summary, corruption consists in a behaviour where a person offers or is solicited, approved or received, promises, gifts or presents, for the purpose of performing or refraining from any act of obtaining favours or specific benefits. Corruption is said to be passive when coming from the corrupt, it is called active when it is the fact of the briber.

Ultimate Beneficial Owner

“Ultimate Beneficial Owner” (UBO) is defined as person(s) who ultimately own(s) or control(s) the registered user and/or the natural person(s) on whose behalf a transaction or activity is being conducted.

The concept of UBO has three basic aspects to be taken into consideration and the holder of any of such aspects is to be considered as UBO and shall complete this declaration:

1. Ownership: Legally possess, directly or indirectly, the right of property (or partially possess such rights) over the assets, goods, valuables, royalties, rights or any other comprised in the specific relationship.
2. Benefit: Be able to claim or be the ultimate person who profits (or partially benefits) from the assets, rights, good, values royalties or rights or their proceeds.
3. Control: Be granted by right or agreement with the possibility of deciding over the utilisation, assignment or some sort of disposition over the assets, goods, valuables, royalties, rights or any other comprised is the specific relationship.

Politically Exposed Person

“Politically exposed person(s)” refer to natural persons who are or have been entrusted with prominent public functions (and immediate family members or persons known to be close associates of such persons) and who are acting outside of the frame of the entrusted duties applicable to such functions.

The relevant regulations include some examples of such functions and the relationship which

will provide them the status of PEP or close associate.

For further details on the treatment of structures involving a PEP and the identification of PEP, please contact the CO.

Shell Bank

"Shell bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

Risk Based Approach

The "Risk Based Approach" (RBA) refers to the decision to apply a specific rule to a situation as a result of an assessment of the potential risk involved in the same and considering the obligations imposed by rules and regulations applicable at the time of such assessment.

Risk Assessment

A "Risk Assessment" is the collection and analysis of relevant data in order to produce and objective profile of a person, entity, jurisdiction, product or situation, with the aim of understanding the risk involved in the relationship.

The scope of a risk assessment is limited to the type of risk that such assessment explicitly mentions to have taken into consideration.

Equivalent Jurisdictions

An "Equivalent Jurisdiction" is a jurisdiction considered as having AML/CTF laws and regulations similar in their content to the ones contained in the relevant regulation.

WHISTLE-BLOWER

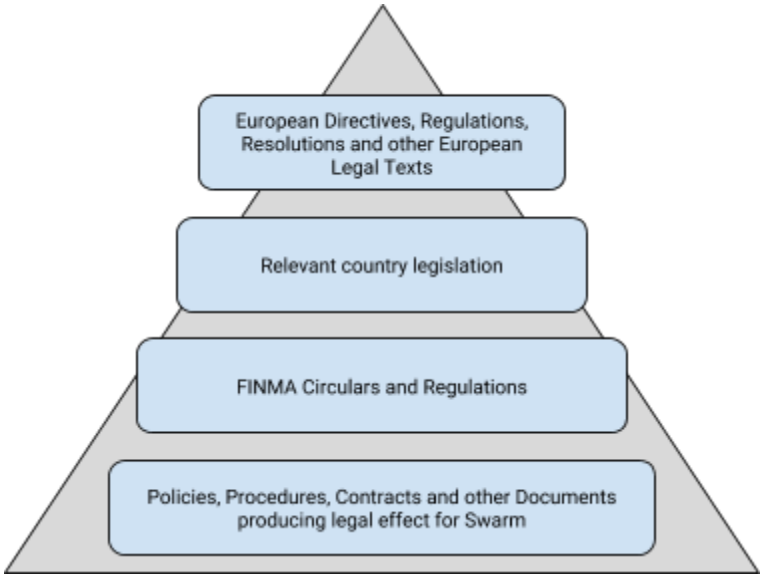
"Whistle-Blower" is a person who reports a wrongful, unethical or unlawful behaviour, misconduct internally or externally.

Relevant Current Rules and Regulations

Following European hierarchy of relevant rules and regulations, the following is a summary of laws and regulations, which can be replaced or amended by relevant authorities without the

immediate need to update the policy unless a new obligation, a stricter requirement or a further provision calls for such update.

Rather than focusing on replicating the content of existing laws, the present policy aims to explain the relevant obligations and company's reinforcements of the professional obligation applicable to Swarm and its staff members. The adjacent graphic should show an overview of the individual legal elements as well as their context, hierarchy and dependency.



European Directives and Regulations

- 1st Anti money laundering Directive, (91/308/EEC) as amended,
- 2nd Anti money laundering Directive, (2001/97/EC) as amended,
- 3rd Directive Anti money laundering, (2005/60/EC) as amended,
- 4th Directive Anti money laundering, (2015/849/EC),
- AML Regulation (2015/847/EC).

Swiss Laws and Regulations

- Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (955.0)
- Verordnung der Eidgenössischen Finanzmarktaufsicht über die Verhinderung von Geldwäscherei und Terrorismusfinanzierung (955.033.0)
- 2011/01 FINMA-Rundschreiben "Tätigkeit als Finanzintermediär nach GwG" (20.10.2010)
- Regulations of the Self-regulatory Organisation pursuant to the Anti-Money Laundering Act VQF Financial Services Standards Association regarding the Combating of Money Laundering and Terrorist Financing (Version: 28 September 2015)

U.S. Laws and Regulations

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“USA PATRIOT ACT”)
- Various statutes, regulations and Executive Orders administered by the U.S. Department of the Treasury Office of Foreign Assets Control (“OFAC”) and the Foreign Corrupt Practices Act (“FCPA”).

Financial Action Task Force

On a quarterly basis the FATF produces statements highlighting AML related issues which include the list of jurisdictions presenting a higher risk for ML and it is anticipated that in the future such statements will be extended to jurisdictions with issues regarding the control of TF.

Such statements and subsequent circulars or regulations produced by Swiss authorities for local implementation are a dynamic part of this procedure and are to be considered as integral part of the same.

From time to time, the FATF amends or revise the current list of recommendation to be followed at international level, whenever this occurs, new rules and regulations may be produced in that sense.

Personal Responsibility

Every staff member of Swarm is responsible for the fight against money laundering, the counter of terrorist financing, the detection and exposure of corruption acts and therefore all staff members are to follow this policy, to inform supervisors or the Compliance Officer regarding any activity potentially linked to the actions mentioned herein and if no action is taken, staff members are encouraged to be a whistleblower in protection of the market.

To receive a copy of the aforementioned legal texts or regulations, as well for a latest version of each regulation, please contact the Compliance Officer (CO) for further details.

Every single employee, affiliate or foundation council member of Swarm has the responsibility of complying with the law, policies and procedures, in specific with AML/CTF/KYC and Counter corruption related areas, as well as the legal obligation to use their knowledge for the avoidance of been involved or facilitate the use of Swarm in the financing of any illegal action, but in particular the ones cover under the scope of this policy.

According to specific hierarchy levels, tasks and responsibilities, different staff members will perform different tasks and will commit to further responsibilities in order to ensure compliance, to protect the firm and to protect the financial market.

The ultimate responsibility for compliance sits with authorised management, daily management, heads of department (referred herein as senior management), the board of directors and the investors of Swarm according to the scope of the decision made.

This responsibility does not include the individual responsibility of each member of Swarm staff, nor responsibilities assigned to third parties when the relevant regulation appoints or admits the

transfer, partial, limited or total of such responsibility(ies).

List of roles, tasks and responsibilities related to the joint fight against ML, TF and Corruption:

- All staff members shall observe this policy and when applicable report to superiors or the CO of any conduct which could potentially harm Swarm,
- Client facing staff are the first line of protection of Swarm and it is up to them to provide information, use their knowledge and help in the prevention of criminal activities taking place in connection to Swarm or its employees,
- Control functions are to communicate with client facing persons and to verify the information/document provided in order to ensure coherence and to serve as a second line of defence,
- Risk and Compliance are responsible to communicate potential risk, to provide advice to senior management to perform an enhanced oversight in order to raise alerts and to stimulate compliance awareness and compliance in decisions made by senior management and directors,
- Senior management and directors are ultimately responsible for business conduct and shall ensure compliance when taking decisions,
- Internal audits work as a further line of defence in order to verify that controls, procedures and conducts were taken according to the expected and effective guidelines,
- External audits perform enhanced protection, vigilant to all the procedures and conducts performed by all internal parties,
- The regulator is there to produce effective measures in order to limit risk appetite, in particular when such risk puts in danger the stability of the system or the transparency and fairness of the market, and to take actions when participants fail to comply with the rules and frameworks established.

Professional Obligations

In jurisdictions Swarm is dealing with the laws, rules and regulations include a number of professional obligations which Swarm follows. Those obligations include:

1. A Risk Based Approach and a Risk Analysis,
2. Vigilance obligations, including Customer Due Diligence (CDD),
3. Implementation of an appropriate internal organization, internal and external auditing, the creation of a compliance culture, an awareness and training program,
4. Cooperation with authorities and regulators.

In development of such professional obligations, Swarm performs the following controls, risk identifiers, risk mitigation plans and specific measures (as applicable):

Risk Based Approach and Risk Analysis

No activity or service can be considered risk-free if it operates in an economic environment and has access to markets. Understanding the conditions of the market and the risk profile of the targeted clients of Swarm, certain activities will be performed in the frame of a RBA, in which main risks such as risk of ML, TF or corruption will be analysed from a regulatory perspective

and from a reputation based approach.

This analysis will be a collection of factors that together with the services provided, may generate mitigation actions and other action plans as considered appropriate by senior management. The analysis of the specific risk applicable to a business relationship may generate a further level of control, a specific action or a number of operations which will represent the mitigation of the detected risk. Every time that a particular risk related to a product or a business relationship appears, the same will be analysed in order to see the potential impact of such risk and if needed to create an action plan. The risk level should be in line with the level of due diligence applied and the depth of knowledge of the client.

Customer Due Diligence

Due diligence refers to the information and documents required to properly identify the user and will be in line with the legal requirements for the verification of the information provided. The basic types of Due Diligence are:

1. Simplified Due Diligence: Set of reduced measures aimed to properly identify a client whenever the risk has been deemed as low and the legal and regulatory conditions to apply such reduction are met,
2. Enhanced Due Diligence: Set of measures aimed to properly identify a client whenever in presence of risk factors requiring a deeper knowledge of the client or when a legal and regulatory provision requires such measures.

The following table gives an overview of the correlation between risk and the level of due diligence applicable which may vary according to several considerations. A field marked with “x” means that this combination is excluded by relevant regulations; a field marked with “+” means that this combination is applicable if conditions set in the relevant regulations are met.

	Low Risk Level	High Risk Level I	High Risk Level II
Simplified Due Diligence	+	x	x
Enhanced Due Diligence	+	+	+

The specific measures to be taken in a case-by-case base will vary in accordance with the specificities of the case but in no event, will go against the prohibitions set in the table above. For more detailed information, please refer to the CO.

Performance, Timing, Updating and Documentation of CDD

CDD refers to the identification and verification of identity of clients, beneficial owners, representatives, relevant related parties and the identification of potential relevant risks affecting the business relationship. According to the risk level, CDD can be simplified, standard or enhanced.

Performance of CDD

CDD implies the obligation of collecting information and documents relevant to client identification, rating of the client and the business relationship.

For this purpose, Swarm has put in place a series of systems, teams and tools for gathering and analysis of information and documents aimed to create a client profile. To achieve this aim, the following should be considered:

1. Identifying and verifying the client's identity on the basis of documents, data or information obtained from a reliable and/or independent source, as applicable, according to the risk level of the customer and the type of due diligence required. Such information/documents may vary on a case-by-case basis but at all times should provide comfort regarding the understanding of the client, structure, beneficial ownership and profile as applicable,
2. If UBO(s) is/are identified, relevant documents and pieces of information shall be gathered in order to clearly identify and verify the identity of such person/people in accordance to the risk level and the type of due diligence to be applied in each case,
3. Obtaining information on the purpose and intended nature of the business relationship as well as determining whether the client is acting on its own behalf or on behalf of a third party
4. Conducting ongoing monitoring of the business relationship including scrutiny of transactions (when the nature of the services provided involve transactions) undertaken throughout that relationship to ensure that the transactions being conducted are consistent with the acquired client knowledge, its commercial activities and risk profile, including, where necessary, the source of the funds and ensuring that the documents, data and information held are up-to-date.

In accordance with the relevant regulation, due diligence should be performed in all cases and will include the above-mentioned elements.

When the client identification process cannot be duly completed, Swarm employees or subcontractors should:

- Not engage into a business relationship,
- Not execute the transaction,
- End the existing business relationship,
- Stop the internal process of client acceptance and continuance,
- Consider notifying the CO to initiate a potential communication with the VQF (please see "Cooperation with the authorities" chapter).

Timing of CDD

Clients evolve and change over time. In order to respond to this reality, Swarm adapts its systems to react to new information, documents or relevant finding both for the acceptance and continuance of client relationships.

To ensure that relevant information and documents correspond to the current situation of the

client, CDD must be performed or updated according to a number of rules which are described here below:

1. When establishing a business relationship,
2. A CDD must be applied on all users registering, independently of the amount Involved,
3. At any time based on a risk assessment (e.g. in the event of high risk criteria occurring, significant transactions performed, etc.)
4. When there is a suspicion of ML or TF
5. When there are doubts about the veracity or adequacy of previous obtained user identification data.

The CDD must be applied to all registered users, i.e. all users for which we have currently at least an open User Account and to all types of services independently of the fees applied.

The user acceptance process involves the identification and the verification of the identity of the registered user, where applicable the UBO, and must be finalised before engaging into a business relationship as per the applicable law in accordance with to the pre- assessed risk level.

The purpose of the business relationship and the determination of whether or not the client is acting on its own behalf is an integral part of the CDD.

Any exception to this rule should be explicitly contained in the relevant regulation and the decision to apply such provision should be documented in the client's file.

Updating CDD

In respect of the professional obligations of the company, user information (and relevant verification documents) should be kept up-to-date.

The compliance of the client file shall be reviewed in accordance to the following cycle of reviews or whenever new information comes to the knowledge of the engagement team:

- High risk II clients' files have to be reviewed on an annual basis,
- High risk I clients' files have to be reviewed every 2 years,
- Low risk clients' files have to be reviewed every 3 years.

Triggering facts which may prompt a review (and further update if necessary) of the client's file include:

1. New relevant information comes to the knowledge of the client relationship team,
2. When considered appropriate by the MLRO or by a senior management decision,
3. When the circumstances of the service or further services require an update of the information on file.

Documentation of CDD

The user acceptance and continuance process has been developed to analyse and store the result of the analysis of KYC, AML, CTF and relevant risk rating, knowledge and data as well as to document the formal acceptance of each client based on various.

This tool groups together a number of systems which integrate and cooperate in the client acceptance and client continuance process as well as interact with different working tools used by relevant teams.

Monitoring of Users

As part of the monitoring process of CDD, teams are required to perform the necessary duties and conduct business in compliance with applicable laws and regulations.

Sanction and name screening are integral part of the client acceptance process as well as the monitoring of clients. Therefore, the company provides the necessary tools and systems to ensure such control at all times.

Transactions considered out of the profile of the client will be scrutinised, analysed and submitted for senior management approval.

In this case, regardless of the decision to perform or reject the operation, documentation of the decision shall be stored in the appropriate software for control of documentation.

Operations, transactions or orders which raise a reasonable doubt of being linked with corrupt acts, money laundered or financing of terrorism should be brought to the attention of the CO for further analysis.

In case a Suspicious Activity Report (SAR) is filed (or to be filed), please refer to the appropriate section of this policy and please make specific attention to the criminal and civil implications delivered for not following the channels of communication and secrecy specified for the situation.

Swarm employees and directors are hereby made aware of the statutory obligation to not disclose to the client, a third party or any non-authorised party partial or complete information related or connected to a potential SAR or the process of the analysis of the appropriateness of such reporting. This limitation cannot interfere with the cooperation with authorities, nor with the functions and attributes of the CO and support team.

Complex Operations or Unusual / Suspicious Activities

The ongoing monitoring duty implies the detection (according to the services provided) of complex operations or unusual / suspicious activities by taking into account:

- The size of the amounts involved,
- The type of users,
- Their profile,
- The information available,
- Other factors considered as relevant by the technical team.

The level of understanding of the transactions will be determined by the specific services provided and in accordance to the access to the information required to perform such service.

Whenever there is a potential suspicion regarding a client, activity or transaction, reference is made to the guidelines laid down in the appropriate section (Cooperation with authorities).

AML / CTF Blacklists, Sanctions, Control and PEP Lists

The names of registered users, UBOs, and appropriate related parties shall be screened using the tools provided by Swarm and the resulting analysis and documentation of this process is to be considered as part of the Client Acceptance process.

Additionally, an automatic system is in place to ensure monitoring and to trigger a re-assessment of the registered user and a potential update of the file as applicable.

The name screening system is updated regularly with the latest information provided by the service provider in cooperation with the provider of the tool to handle potential matches.

Swarm might create a series of internal lists which will not necessarily mean the imposition of a sanction, blacklisting or any other restrictions and therefore the actions related to such list will be documented according to internal practice.

In case of a match, the engagement team in cooperation with CO will perform the appropriate investigation to determine whether it is a real match or a false positive. In case of real match, an assessment should be produced and documented in order to determine further actions to be taken.

Prohibited and Refused Relationships

In the cases in which the relevant regulation prohibits entering into business relationship with a user or a type of user, Swarm will not accept the user and will refrain from performing transactions with such prohibited individual or entity. As a matter of example, it is prohibited to establish or maintain a business relationship with shell banks.

Whenever a decision to refuse a user is made, the Swarm authorised management of the respective Line of Service should be made aware. The Swarm authorised management will inform the CO on this event and provide the reasons of such refusal.

The CO should keep a log of all prohibited and refused business relationships together with the reasons for such refusal.

Cooperation with Authorities

Swarm will respond to a request (“Request”) concerning User Accounts and transactions by immediately searching our records to determine whether we maintain or have maintained any User Account for, or have engaged in any transaction with, each individual, entity or organisation named in the Request.

We will designate one or more persons to be the Point of Contact (PoC) for Requests and will promptly update the PoC information following any change in such information.

Unless otherwise stated in the Request, we are required to search our files for each individual, entity or organisation named in the Request.

If we find a match, the CO will consider any appropriate action. If the search parameters differ from searching through our entire database, for example, if limits to a geographic location apply, the CO will structure our search accordingly.

If the CO searches our records and does not find a matching account or transaction, then the CO will not reply to the Request.

We will maintain a register of ML and TF Enquiries together with documentation that we have performed the required search by saving the logs, which will at all times be available on request.

Swarm will direct any questions about the Request to the authorities and not disclose the fact that the authorities have requested or obtained information from us, except to the extent necessary to comply with the Request.

The CO will review, maintain and implement procedures to protect the security and confidentiality of requests from the authorities with regard to the protection of customers' non-public information.

Unless otherwise stated in the Request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the Request as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

Whistle Blower Policy

Whenever any staff member comes to the conclusion that it is worth informing to Swarm ay of the potential situations under the whistleblower definition in the procedure, the person is encouraged to follow the disposition contained in this chapter and any applicable rules and regulations.

Swarm encourages employees and staff members to follow up on the situations and potential risk brought to the attention of the CO.

Limited by the confidentiality and secrecy rules applicable to the steps, decisions and operations of the escalation of suspicious activities, if employees are aware that no action was taken in regards to a situation worth to be brought to the attention of authorities, they may use their legal right and obligation of acting as a whistle blower.

Before bringing to the attention of any third party any situation, employees should attempt to raise the issue internally in order to allow the responsible person to take actions in the matter.

Employees which happen to detect a corrupted action or a facilitation of ML or TF within Swarm shall immediately report the situation to the CO or the board of directors for disciplinary actions and to immediately create applicable action plans and controls to bring the situation under control and to comply with applicable laws and regulations.

The encouragement and protection of whistleblowers cannot conflict at any point with the general obligations of labour law, professional secrecy and should be always aligned with the principles of bona fides and shall provide Swarm with the option of taking actions against any potential breach which is not clearly defined as structural and official company conduct.

Internal and External Controls and Audits

Swarm has set a number of internal controls and assessments. To ensure the commitment of Swarm with regulatory requirements, ethical behaviours and controls, Swarm has created a

3-layered control system. Swarm has put in place a team of specialists in order to fulfil every process or system provided by a third party and better fulfil and further comply with regulatory and Swarm expectations.

The 3-layered process can be described as follows:

- Layer 1 - Swarm Operations Team, the first checkpoint to decide which rules and regulations are required,
- Layer 2 - Swarm Risk and Compliance team
- Layer 3 - Swarm Internal Audit

For specific matters Swarm may call upon professionals to assist in the better structuring and fulfilment of the compliance commitment and compliance culture.

Ongoing Training, Recruitment and Awareness

Swarm employees and collaborators are required to participate in ongoing training programs related to AML and CTF. The training and awareness program must include a regular ongoing training program addressing particularly, but not exclusively, user on-boarding and order processing staff and to the staff in charge of AML and CTF compliance. The purpose of the program is to inform or remind relevant staff about the up-to-date status of the following topics:

- Swarm's AML and CTF procedures,
- Different aspects of the laws and duties regarding AML and CTF,
- Professional Standards related to AML and CTF,
- Examples of operations susceptible of being linked to ML or TF and instructions how to proceed if a suspicious case is indicated.

According to the function, the staff will be trained and made aware of the applicable AML and CTF regulations and duties.

Participation in Training Program

Swarm will use appropriate channels to distribute information and raise awareness regarding AML and CTF matters. Relevant employees and collaborators (subcontractors, contractors, third parties, etc.) of Swarm are to undertake training on yearly basis. For employees, specific Swarm training will be provided, while for collaborators there will be the option to provide Swarm with evidence or comfort regarding such training.

Recruitment

Potential candidates will be required to agree to a screen of their names against black and control lists. Additional parts of the process can be externalised and reports shall be presented by the service provider.

If the activity of on-boarding of personnel happens to be performed by Swarm directly, this will be done in subjection to relevant labour, anti-money laundering and applicable legislations.

Employees will be requested to follow necessary steps, controls and actions required by laws and regulations applicable at the time and additionally will be requested to provide a police

clearance certificate from the countries in which they have resided in the last 3 years' prior their candidature.

Every new staff member will be presented with the necessary policies and provided with relevant training in matters applicable to their position within the first 3 months from the first day of effective work. The failure to comply with the above from the new staff member is a serious labour misconduct which may result in termination of the working contract.

Document Retention

All documents related with Client Acceptance and Continuance will be kept for a period of ten (10) years from the end of the business relationship with the user or after the date in which the occasional transaction was performed.

Exceptionally, Swarm may store the information and supporting documents for a longer period due to specific potential risk characteristics of the client or the relationship as per decision of the CO.

Personal data for persons of contact, including service providers, contractors, employees and other will be kept for the same period. Other information will be kept based on the applicable law and regulation for that matter to the maximum foreseen by the law and in accordance with the paragraphs above.

If no other information is giving by relevant rules and regulations the ten (10) years' document retention policy should apply.

Policy Compliance

Compliance Management

The responsible security officer will verify compliance to this policy through various methods, including but not limited to, internal and external audits, and feedback to the policy owner.

Non-Compliance

An employee found to have violated this policy may be subject to severe consequences including disciplinary action that may trigger various sanctions depending on the nature of the violation. Sanctions may range from notification that will stay in the employee's file to dismissal in case of severe violation and repeating offenses.

Update and Approval

The present policy should be revised annually and updated whenever appropriate. For updates in citation, and not material changes the update can be performed immediately with the double approval of the CO and one authorised manager of Swarm. For further or material updates or modifications, this will be presented to the board of directors for approval. In yearly bases, all changes will be presented to the board of directors for their final approval, or in case in which during a year no change was performed, this situation will be brought to the attention of the board of directors.

Validity and Document Management

This policy and procedure has been approved by Swarm board of directors on 5 November, 2018. It replaces and supersedes any prior policy and procedures on this subject matter. This policy is valid until a revision is published.

DATE OF APPROVAL BY FOUNDATION COUNCIL	APPROVED BY	VERSION	SIGNATURE
INSERT DATE	Board of Directors	1.0	