



**Anti-Money Laundering and Counter-Terrorist Financing
Policy and Procedures**

Date of issuance : 1 January 2024
updated :

Table of contents

1	Introduction	3
2	Scope of application.....	3
3	Key concepts	3
4	Due diligence and ongoing vigilance on Investees.....	4
4.1	Investee due diligence	5
4.1.1	Identification of the Investee, its agent(s) and UBO(s)	5
4.1.2	Verification of the identity of the Investee, its agent(s), and UBO(s)	5
4.1.3	Identification of the characteristics of the Investee, its agent(s), and UBO(s).....	5
4.1.4	Individual risk assessment of the Investee.....	6
4.2	Ongoing due diligence	7
5	Acceptance policy	7
6	Organisational measures.....	8
6.1	Governance.....	8
6.2	Data and document retention	8
7	Policy updates	9
	Annex 1 – Ultimate Beneficial Owners.....	10
	Annex 2 - High-Risk Third Countries.....	11
	Annex 3 - Tax Havens.....	11
	Annex 4 - Politically Exposed Persons	11

1 Introduction

As a listed company, TINC is committed to upholding high standards of transparency, integrity, and ethical conduct. As part of that commitment, we recognise the importance of preventing money laundering and the financing of terrorism. Even though we are not legally obliged to adhere to antimoney laundering and counter-terrorist financing (“**AML/CTF**”) laws and regulations, complying with those laws and regulations is part of our responsible investment principles, as set out in our Sustainability Policy. Therefore, in the spirit of maintaining the trust of our stakeholders and taking responsibility in safeguarding the financial system from illicit activities, we voluntarily commit to complying with AML/CTF principles.

Some of the requirements set out in AML/CTF laws and regulations are hard to reconcile with the activities of TINC as an investment company. For instance, as TINC does not carry out transactions on behalf of customers, it would be disproportionate to implement a transaction monitoring system or to investigate suspicious transactions. Rather than implementing all the requirements set out in AML/CTF laws and regulations, our intention is to integrate AML/CTF principles and standards into our investment processes, with a view to ensure that we implement a responsible standard of due diligence when allocating investment money to companies or projects (hereinafter referred to as “**Investees**”).

In light of the above, the objective of this policy and the procedures set out herein (together referred to as “**the AML/CTF Policy**” or “**this policy**”) is to offer assurance that we do not allocate funds to Investees where we suspect, know, or are reasonably expected to know, that they, their agents, or their ultimate beneficial owners (“**UBOs**”) engage in money laundering or terrorist financing.

2 Scope of application

This policy applies to all investments carried out by TINC (hereinafter “**the Company**”), whatever their legal nature (*e.g.*, equity or debt transactions). This policy must be complied with by all individuals working at all levels within the Company and its external service providers responsible for the management of the Company (i.e. including directors, managers, employees) (together referred to as “**the Staff**”), whether working part-time or on a fixed-term basis and whether working from home or on site.

This policy shall be communicated to all Staff members and shall be readily accessible at all time, *e.g.* on the intranet and/or common drives.

3 Key concepts

The following are key concepts in the context of anti-money laundering and counter-terrorist financing rules:

- **AML/CTF**: Anti-Money Laundering and Counter-Terrorist Financing;
- **High-Risk Third Country**: a jurisdiction that poses a higher risk of money laundering or terrorist financing activities (see Annex 2) ;
- **Money laundering**: either of the following actions:

-
- the conversion or transfer of money or other property, knowing that this is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of his action;
 - the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of money or property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
 - the acquisition, the possession or the use of money or property, knowing, at the time of receipt, that these were derived from criminal activity or from an act of participation in such an activity;
 - participation in, association to commit, attempts to commit and aiding, abetting, facilitating or counselling the commission of any of the actions referred to under 1°, 2° and 3°;
- **Politically Exposed Person (“PEP”)**: individuals who hold or have held prominent positions in a government or public administration, as well as their immediate family members and close associates (see annex 4);
 - **Sanctioned Individual**: any natural person, legal entity or organisation mentioned on a list of financial sanctions applicable in Belgium;
 - **Tax Haven**: jurisdictions that impose minimal or zero taxes on certain types of income or entities, and which present increased risks for money laundering due to a lack of transparency and/or cooperation on fiscal matters (see annex 3);
 - **Terrorist financing**: the provision or collection of funds and other assets, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, by a terrorist organisation or by a terrorist acting alone, even without any link to a specific terrorist act.

4 Due diligence and ongoing vigilance on Investees

The purpose of the due diligence and ongoing vigilance measures set out herein is to obtain reasonable assurance that an investment does not expose the Company to the risk of invested funds being used for purposes of money laundering and/or terrorist financing. To that end, these measures seek to collect a minimum of information to be able to make an informed judgment on the financial crime risks related to an Investee (“**individual risk assessment**”). The outcome of that assessment must be communicated to the Management Board *c.q.* Supervisory Board with a view to enabling it to integrate financial crime risks in its ultimate investment decision. The acceptance policy set out herein (see 5 below) determines how the Management Board should take into account the outcome of the individual risk assessment in its decisions on investments.

The due diligence and ongoing vigilance measures shall be applied throughout, and in addition to, the Company’s regular investment due diligence processes.

4.1 Investee due diligence

Due diligence on Investees shall include the identification of the Investee and the verification of its identity, as well as of its agent(s) and UBOs, in accordance with the standards set out herein. That requires (i) the collection of relevant information to be able to distinguish those persons from any other person with reasonable certainty (“**identification**”), and (ii) the verification of all or part of the identification data against one or more supporting documents or reliable and independent sources of information which enable the data to be confirmed so as to have a sufficient degree of certainty as to the identity of the persons involved (“**identity verification**”).

4.1.1 *Identification of the Investee, its agent(s) and UBO(s)*

Before allocating funds to the Investee the Company shall collect the identity information of the Investee, its agent(s), and its UBO(s) (annex 1 to this policy provides a detailed overview of the persons that must be considered UBOs and thus identified in accordance with this policy).

The Company shall appoint a person among its Staff as a responsible for collecting the identity information and keeping a record thereof (hereinafter the “**AML record**”).

For the purposes of this policy, that Staff member shall hereinafter be referred to as the Due Diligence Officer, or “**DDO**”).

4.1.2 *Verification of the identity of the Investee, its agent(s), and UBO(s)*

In order to obtain a sufficient degree of certainty as to the identity of the persons involved, The DDO shall verify the identity of the Investee, its agent(s), and its UBO(s) by comparing the collected identity details to one or more supporting documents or reliable and independent sources of information that can confirm the accuracy and reliability of the identity information and keep a record thereof.

In case of a discrepancy between the identity information previously collected and the identity information recorded in the verification documents, the DDO shall request the Investee to correct the previously submitted information and to give an explanation for the discrepancy, which must be plausible and substantiated by supporting documentation (*e.g.*, in case of a recent change in corporate details that has not yet been published, a discrepancy can be justified by the submission of a recent notarial deed confirming the change of information). The explanation and supporting documentation.

4.1.3 *Identification of the characteristics of the Investee, its agent(s), and UBO(s)*

Before deciding to invest in an Investee, the Company shall identify a number of characteristics of the Investee. The identification of those characteristics is necessary to allow the Company to (i) understand potential financial crime risks related to the Investee, and (ii) integrate its understanding of those risks into the Management Board’s *c.q.* Supervisory Board’s final decision to allocate funds to the Investee.

Based on the verified identity details of the Investee, its agent(s), and its UBO(s), the DDO identifies the following characteristics such as:

- whether the Investee or its agent(s) or its UBO(s) is incorporated or is established in (i) an EEA country, (ii) a non-EEA country, (iii) a High-Risk Third Country or (iv) a Tax Haven, by

comparing the identified country of incorporation against the list of High Risk Third Countries and Tax Havens set out in the Annexes to this policy;

- whether the Investee, the agent(s), or the UBO(s) are a Sanctioned Individual or a PEP according to available sources.

The DDO shall obtain proof of consultation of the relevant external sources and record a copy thereof in the AML record of the Investee.

4.1.4 Individual risk assessment of the Investee

Based on the identified identity details and characteristics of the Investee, the DDO carries out an individual risk assessment of the Investee. The purpose of that risk assessment is to offer a clear indication of the financial crime risks related to the Investee, which the Management Board *c.g.* Supervisory Board must take into account upon its final decision to proceed with the investment (see 5 below).

The individual risk assessment shall be carried out as follows. The DDO shall allocate a risk score to different risk factors in accordance with the table below. The Investee's final risk class shall correspond to the highest score allocated to either of the applicable factors.

The DDO shall document the individual risk assessment by filling out the table below for each Investee and keeping a copy of the completed table under the Investee's AML Record.

Risk factor	Scoring criteria	Risk score	Risk class
1° Country of incorporation of the Investee	EEA country	0	Low
	Non-EEA	1	Medium
	High-Risk Third Country	2	High
	Tax Haven		
2° Country of incorporation or residency of (one) of the agent(s)	EEA country	0	Low
	Non-EEA	1	Medium
	High-Risk Third Country	2	High
	Tax Haven		
3° Country of residency of (one) of the UBO(s)	EEA country	0	Low
	Non-EEA	1	Medium
	High-Risk Third Country	2	High
	Tax Haven		
4° The Investee, its agent(s), and/or its UBO(s) are a Sanctioned Individual	No	0	Low
	Yes	3	Very High
5° The Investee, its agent(s), and/or its UBO(s) are a PEP	No	0	Low
	Yes	2	High
6° The Investee, its agent(s), and/or its UBO(s) are subject to adverse media	No	0	Low
	Yes	2	High

4.2 Ongoing due diligence

The DDO shall update all due diligence information on the Investee, including the verification documents and risk assessment, whenever there are indications that a change in the status may have occurred. That update shall be documented and record in the Investee's AML record. In the event of a change that affects any of the risk scores of the Investee, the DDO shall immediately notify the Management Board of the Company.

4.3 Divestment

In the event whereby the Company would receive money from third parties in the context of a divestment of an Investee, the same principles as set out under this section 4 shall be applied *mutatis mutandis* with respect to third parties involved in such divestment process from which the Company should receive money.

5 Acceptance policy

The purpose of the due diligence measures set out in this policy is to offer reasonable assurance to the Management Board *c.q.* Supervisory Board regarding the financial crime risks involved in an investment decision.

Before making an investment decision, the Management Board *c.q.* Supervisory Board shall consult the AML record of the Investee. In particular, the Management Board *c.q.* Supervisory Board shall take note of the individual risk assessment and the risk class of the Investee, as documented in the risk assessment table prepared by the DDO.

Depending on the outcome of the individual risk assessment, and in particular the risk class of the Investee, the Management Board *c.q.* Supervisory Board shall take the following actions:

- If the risk class is "Very High", the Management Board *c.q.* Supervisory Board shall not under any circumstances allocate funds to the Investee.
- If the risk class is "High", the Management Board *c.q.* Supervisory Board shall give due attention to the specific risk factors that underpin the risk class and shall, in case of a positive investment decision, include an explicit motivation as to the acceptance of the potential financial crime risks in the meeting minutes.
- If the risk class is "Medium", the applicable risk factors that underpin the risk class must be formally acknowledged by the Management Board *c.q.* Supervisory Board.
- If the risk class is "Low", there are no specific financial crime risks to be taken into account by the Management Board *c.q.* Supervisory Board, unless the Management Board *c.q.* Supervisory Board has received information to the contrary through channels or due diligence measures other than those foreseen by this policy.

6 Organisational measures

6.1 Governance

The Company adopts the following AML/CTF governance structure, which clearly allocates responsibilities to each of their governing bodies and functions, along with control mechanisms to ensure that the respective persons within the Company effectively perform their AML/CTF-related tasks.

The Management Board, in the supervision of the Supervisory Board is responsible for :

- i. deciding on the overall AML/CTF risk management strategy of the Company;
- ii. approving and modifying this AML/CTF policy;
- iii. for the execution of the AML/CTF risk management strategy of the Company and for ensuring the implementation of this policy.

The Management Board shall appoint one person among its members as a manager for AML/CFT (hereinafter “**AML Manager**”), responsible for:

- i. raising awareness among the entire Management Board for AML/CTF risks;
- ii. ensuring that this AML/CTF policy, procedures and internal control measures are adequate and proportionate, taking into account the Company’s characteristics; and
- iii. ensuring the appointment of a DDO ;
- iv. monitoring compliance with the AML/CTF policy

The role of AML Manager is entrusted to the Compliance Officer.

6.2 Data and document retention

The Company shall retain the following information and documents in individual AML records for each Investee:

- the collected identity information of the Investee, its agent(s), and their UBO(s), including any updates to that information;
- the documents used to verify that information, including any updated versions;
- the results of consultations of external sources of information;
- the documentation of the application of the due diligence measures set out herein, such as the completed individual risk assessment tables.

The information and documents shall be retained for a period of 5 years counting from the end of the contractual relationship with the Investee. the Company shall delete all information at the end of the retention period. the Company shall ensure that its privacy policies enable the GDPRcompliant processing and retention of personal data that are required by this policy.

7 Policy updates

This policy shall be updated regularly.

Annex 1 – Ultimate Beneficial Owners

The Company shall identify the UBOs of its Investees and their agents (to the extent that agents are not natural persons). The UBOs are the natural persons who ultimately own or control the Investee and its agent(s).

Depending on the legal form of the Investee or agent, the following persons shall be identified as UBOs of the customer or agent:

Legal form of customer or agent	UBO
<p>Corporate entity</p> <p><i>Examples:</i></p> <ul style="list-style-type: none"> - BV/SRL - NV/SA - CV/SC - CommV/SComm - VOF/SNC - SE - SCE 	(i) any natural person holding more than 25% of the voting rights, shares, or ownership interest, either (a) directly in the company concerned itself (“ direct ownership ”), or (b) in one or more entities that, individually or jointly, hold more than 25% of the voting rights, shares, or ownership interest in the company concerned (“ indirect ownership ”); or
	(ii) if no person under point (i) could be identified, any natural person exercising control over the corporate entity via other means (e.g., by holding a majority of the voting rights, shares, or ownership interest in the company concerned); or
	(iii) if no person under points (i) to (ii) could be identified after exhaustion of all possible means of identification, or there is doubt that the person(s) identified under points (i) to (ii) are the UBOs, the natural person(s) holding the position of senior managing officer, provided that there are no grounds for suspicion.
<p>Non-profit organisation, association, or foundation</p> <p><i>Examples:</i></p> <ul style="list-style-type: none"> - VZW/ASBL - IVWZ/AISBL - PS/FP - SON/FUP - Feitelijke vereniging/ Association de fait 	<p>(i) all the persons who are members of the board of directors; and all the</p> <p>(ii) members of the board of directors who are mandated to represent the entity, acting either individually or jointly, on the basis of a representation clause (<i>‘gedelegeerd bestuurder’</i>); and all the persons – whether board</p> <p>(iii) members or not – to whom the day-to-day management and representation of the entity has been delegated (<i>‘dagelijks bestuurder’</i>); and the natural persons or, if these persons have not yet been designated, the categories of natural persons in whose main interest the entity has been established or operates¹; and every other natural person who exercises ultimate control over the entity through other means, such as proxy agreements with persons identified under points (i) to (iv), or factual circumstances (<i>‘feitelijk bestuurder’</i>).</p> <p>(v)</p>

¹ This category of UBOs must be understood as referring to natural persons benefitting from certain advantages, care, or help, from an organisation, for instance refugees or handicapped individuals (see [Explanatory Memorandum](#), p. 107-108).

Annex 2 - High-Risk Third Countries

a. Third countries having strategic deficiencies in their ML/TF regimes

The European Commission has identified a number of countries as having strategic deficiencies in their ML/TF regimes:²

The European Commission regularly publishes updates of the list. The list set out herein must be updated to ensure that it remains in conformity with the list adopted by the Commission, which is available [\[here\]](#).

b. Third countries identified as presenting a high geographic risk

The third countries below are identified by the Financial Action Task Force, the National Security Council, or the Ministerial Committee tasked with coordinating the fight against the laundering of money of illicit origin, as presenting a high geographic risk:

- Blacklisted countries

Blacklisted countries are the countries mentioned in the FATF list of high-risk jurisdictions subject to a call for action (available [\[here\]](#)):

- Greylisted countries

Countries mentioned in the FATF list of jurisdictions under increased monitoring (available [\[here\]](#))

Annex 3 - Tax Havens

Any of the jurisdictions mentioned on the list of states with low or no taxes drawn up by the Ministry of Finance (available [\[here\]](#)):

Annex 4 - Politically Exposed Persons

Any of the following persons shall be considered Politically Exposed Persons (“PEPs”) (available [\[here\]](#)).

² See Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies [2016] OJ L254/1 (as amended). The consolidated version of the Regulation is available [\[here\]](#).