AML Policy

Document ID: CO-01_V1

Owner: Board of Managers

Scope: LCV Lux GP S.à r.l. – all Relevant Persons and AIF investors

Confidentiality: confidential

Drafted by: Benedikt Gansen
Approved by: Board of Managers
Contact: LoKVLux@gimpel-aifm.lu

Contents

Version History and Approval

Date / Document ID	Prepared by	Approved by	Approved on
CO-01-V1	Benedikt Gansen	Board of Managers	11. August 2026

Definitions

Term	Definition
LCV Lux GP S.à r.l.. / the Company	LCV Lux GP S.à r.l. (the Alternative Investment Fund Manager, hereinafter "the Company")
AIF	Alternative Investment Fund, here: Lok Capital V Lux Feeder SCSp
Lok Capital V Lux Feeder SCSp	The Luxembourg special limited partnership (société en commandite spéciale, "SCSp") managed by the Company, investing solely in its master fund
ACRL	AML Country Risk List maintained by the Company
AML law	The Luxembourg Law of 12 November 2004 on the fight against money laundering and terrorist financing as amended
CO / RC	Compliance Officer, appointed intuit personae by the Board of the Company and registered with the CSSF as responsible for the control of compliance with AML/CTF obligations
CTF	Combating Terrorist Financing
Delegate	As per CSSF 18/698: any third party carrying out on behalf of an IFM one or more functions of collective portfolio management or risk management
FATF (GAFI)	Financial Action Task Force on money laundering and terrorist financing
FIU	Financial Intelligence Unit (State Prosecutor; in Luxembourg: Parquet)
High-Risk Country	Country included in the list of high-risk third countries pursuant to Article 9(2) of the 4th AML Directive or designated by FATF as presenting a higher risk, or otherwise considered high-risk in the Company's AML/CTF risk assessment
ML/TF	Money Laundering / Terrorist Financing
PEP	Politically Exposed Person, as defined under Article 1(9) of the Money Laundering Act
RBA	Risk Based Approach
Red Flag	An obvious indicator which clearly suggests that money laundering, terrorist financing or a predicate offence is occurring or is likely to occur
RR	The management body of the Company, registered with the CSSF, responsible for compliance with AML/CTF obligations
SAR	Suspicious Activity Report – Report to be filed by the CO to authorities on suspicion or knowledge of activity linked to money laundering, terrorist financing or predicate offences
Shell Bank	A credit institution or financial institution incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group

SoF	Source of Funds – the transmission path of the funds received by the Company
SoW	Source of Wealth – how the funds were earned or generated
UBO	Ultimate Beneficial Owner
Well-Informed Investor	An investor as defined under Luxembourg law (Part II UCI / RAIF / SIF regime), being an institutional investor, professional investor, or any other investor who has declared in writing that they are a well-informed investor and either invests a minimum of EUR 125,000 or has obtained an assessment by a credit institution, investment firm or management company certifying their expertise, experience and knowledge

1 Purpose and Scope

The purpose of this policy is to define all procedures, processes and instructions for LCV Lux GP S.à r.l. (hereinafter "the Company") to enable the Company, its Board of Managers (or equivalent governing body) and all staff members to comply with the Luxembourg Anti-Money Laundering and Counter Terrorist Financing laws, regulations, circulars and standard market practices.

The Company acts as the General Partner (GP) and Alternative Investment Fund Manager (AIFM) of Lok Capital V Lux Feeder SCSp, a Luxembourg special limited partnership (SCSp). The fund follows a feeder fund strategy, whereby its sole investment is a participation in its master fund. The fund targets only professional clients as defined under Luxembourg law.

The AML procedures are designed to assist in lowering the following risks associated with an inadequate or non-existent AML programme:

- Reputational Risk: if the Company becomes known for being associated with money laundering or terrorist financing activities, it would lose the trust and confidence of its investors and counterparties.
- Operational Risk: loss resulting from inadequate or failed internal processes or external events, including weakness in the implementation of procedures, ineffective controls and failure to practise due diligence.
- Legal and Regulatory Risk: the risk of regulatory actions and lawsuits resulting from the failure to observe mandatory AML/CTF laws and regulations.

This Policy is reviewed and updated at least annually and on an ad-hoc basis in case of regulatory changes or incidents. The Policy is approved by the Board of Managers.

2 Regulatory Basis, Reference Documents and Professional Obligations

The legal basis for the fight against Money Laundering and Terrorist Financing is defined in the Law of 12 November 2004 on the fight against money laundering and terrorist financing as amended (hereinafter "AML Law"), which has been amended amongst others by the law of 25 March 2020 implementing the provisions of the 5th European AML Directive (Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU) and last amended by the Law of 29 July 2022. as well as the Grand -ducal regulation dated 1st February 2010 providing details on certain provisions of AML Law (hereinafter "Grand ducal regulation") and the CSSF Regulation No 12 -02 on the fight against money laundering and terrorist financing, as amended (hereinafter "CSSF 12 -02"). Further to the above, there are additional Circulars, Regulations and other texts concerning anti - money -laundering and terrorist -financing in place which are published by CSSF under https://www.cssf.lu/en/regulatory -framework/. For reference, this includes in particular without limitation the following:

- Criminal Code (Article 506-1 and Article 135-5);
- Law of 19 February 1973 (Article 8-1) referring to the selling of medicinal substances and fight against drug addiction;
- Law of 27 October 2010 enhancing the AML/CTF legal framework;
- Law of 19 December 2020 on the implementation of restrictive measures in financial matters;
- Law of 13 January 2019 establishing the Register of Beneficial Owners;
- Law of 10 July 2020 establishing a Register of Fiducies and Trusts;
- EU Regulation 2018/1542 concerning restrictive measures against the proliferation and use of chemical weapons;
- Commission Delegated Regulation EU 2016/1675 identifying high-risk third countries with strategic deficiencies;
- Grand Ducal Regulation of 01 February 2010 ("GDR 2010"), as amended;
- CSSF Circulars: 11/529, 11/528, 13/556, 15/609, 17/650, 17/661, 18/680, 18/684, 18/698, 18/702, 19/732, 21/767, 21/782;
- FIU Documentation on freezing of suspicious transactions and declarations of suspicious transactions;
- National and supra-national risk assessments of money laundering and terrorist financing;
- EBA Guidelines EBA/GL/2024/14;
- Commission Recommendation (EU) 2024/214.

Furthermore, the Company applies the following standards and recommendations:

- FATF Recommendations;
- Wolfsberg Statement on Anti-Money-Laundering Guidance for Mutual Funds and other Pooled Investment Vehicles (March 2006);
- Practices and recommendations aimed at reducing the risk of money laundering and terrorist financing in the Luxembourg Fund Industry, as adopted by ABBL, ALCO and ALFI.

Due to the nature and the content of certain circulars the following ones should be highlighted: The CSSF Circular 17/650, as amended by Circular 20/744 – "Application of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended (hereinafter "AML/CFT Law") and Grand -ducal Regulation of 1 February 2010 providing details on certain provisions of the AML/CFT Law ("AML/CFT GDR") to predicate tax offences". The Circular follows on the criminal provisions laid down in t he Law of 23 December 2016 implementing the 2017 tax reform, which introduces the extension of the money laundering offence to aggravated tax fraud and tax evasion. The new provisions transpose the revised FATF standard and conditions of the 5th AML Directive and extend the list of predicated offences to a new category of serious underlying offences, namely the "tax crimes related to direct and indirect taxes".

Consequently, the Company has to take into account the new predicate tax crimes within the scope of its professional obligations, notably customer due diligence and cooperation with authorities. Circular CSSF 17/661 repealed by Circular CSSF 21/782 on the "Adoption of the joint guidelines issued by the three European Supervisory Authorities (EBA/ESMA/EIOPA) on money laundering and terrorist financing risk factors" outlining additional requirements and providing assistance for the application of simplified and enhanced customer due diligence.

Circular CSSF 18/698 on the "Authorisation and organisation of investment fund managers incorporated under Luxembourg law, Specific provisions on the fight against money laundering and terrorist financing applicable to investment fund managers and entities carrying out the activity of registrar agent" further defines the set -up of the AML/CTF framework within the Company and provides minimum content required to be added to the annual report of the Money Laundering Officer towards the Board of Managers and the CSSF .

The professional obligations include in short:

- To apply customer due diligence (CDD) measures, including identification and verification of the customer, all signatories and all beneficial owners, and obtaining information on the purpose of the business relationship;
- To classify all clients according to the AML risk they represent, fulfilling the requirements of the risk-based approach (RBA);
- To scrutinize certain transactions and activities with particular attention;
- To keep all relevant documentation for a minimum of 5 years after termination of the relationship;
- To maintain an adequate internal organisation and regular training for employees;
- To cooperate with authorities and to notify them in the event of potential and/or actual suspicion of AML/CTF related activity;
- To conduct an analysis of the Company's exposure to AML and CTF.

3 Three Basic Steps in Money Laundering

Money Laundering means any action as defined in Art. 506 -1 of the penal code as well as in Art. 8 -1 of the law of 19 February 1973, as amended, concerning the sale of medicinal substances and measures to combat drug addiction. In practice, money laundering means the processing of proceeds, which have been obtained from an illegal or criminal activity to disguise the identity, source, nature or destination of funds. In case a criminal activity generates substantial profits, the persons involved must find a way to control these funds without attracting attention to the underlying activity or the persons involved. This is achieved by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention. This process is of importance, as it enables the criminal to enjoy these profits without jeopardizing their source. Money laundering is on the one hand side conducted either by knowingly/deliberately participating in the process of money laundering but also by ignoring indicia in the course of unusual or suspicious transactions or behavior. Examples of illegal activities that often involve money laundering are terrorism, drug trafficking, smuggling, arms trading, organized crime, prostitution, kidnapping, human trafficking, robbery, illegal gambling, bribery, fraud and tax evasion.

There are three main recognized phases of money laundering:

1) Placement

The money-launderer places dirty money, into the legitimate financial system, e.g. by making cash deposits at a bank. This stage is particularly risky, since large cash deposits tend to attract suspicion. Criminals use different tactics to mitigate the risk of being detected such as smurfing (splitting the money into smaller amounts) or mixing legal and illegal assets. This phase is not applicable in all cases, as certain criminal crimes (e.g. fraud, corruption or insider dealing) generates benefits directly in the financial system.

2) Layering

Once the funds have entered the financial system the next phase is in the money laundering process is the layering. Here the launderer changes the form of the money, that was initially placed with the aim of wiping out any possible traces of identity, source or nature. This can be achieved, for example, by making numerous transfers between different bank accounts with different accountholders in different jurisdictions, by repeatedly changing currencies, buying and reselling various securities, or by buying high -value goods like houses, cars or precious metals.

3) Integration

At the final stage, the launderer reintroduces the money, now seemingly legitimate, into the financial and economic system (e.g. investing into property, luxury items, business ventures, etc.). Detecting dirty money at this stage is much more difficult as transactions now appear to come from a legal source.

4 Terrorist Financing

Terrorist financing is understood as providing, collecting or receiving funds with the intention that those funds be used for the benefit or purpose of a terrorist group. Such activities may involve funds raised from both legitimate sources (personal donations, charitable organisations) and criminal sources (smuggling, drug dealing, fraud, kidnapping etc.).

In general, there are three stages to terrorist financing: the raising of funds, through either illicit or licit activities; the moving of funds; and the using of funds. Terrorist financing not only involves the direct financing of acts of terrorism, but also the financing of propaganda, recruitment, training, travel, daily living expenses and other operational needs of an individual terrorist or terrorist group. The risk of Terrorism and terrorist financing is classified as medium as per Sub -sector risk assessment (collective investment sector). Further risk increasing indicators could be for example none profit organizations (NPOs) within the fund's register, crowd funding or frequent cash transactions, amongst others.

The risk of terrorism and terrorist financing is classified as medium as per the sub-sector risk assessment (collective investment sector). Further risk-increasing indicators specific to the Company include NPOs in the fund's investor register and high-risk country connections, though these are closely monitored.

5 Ultimate Beneficial Owner (UBO)

A UBO is any natural person who ultimately owns or controls directly or indirectly a legal entity (including by bearer shares) with more than 25% of shares, voting rights or participation in the capital, or by other means. This could also be the case, if the minimum -thresholds defined in the law are not met (currently more than 25% of all shares of a company or other artificial person). If, after exhausting all possible means and provided there are no grounds for suspicion, no person can be identified, any natural person who holds the position of senior management official will be considered as UBO, as per the DBO Guidelines of the RBE Luxembourg.

In the case of the SCSp structure, the following persons must also be identified:

- The general partner (GP) and its UBOs;
- The limited partners (LPs) and their UBOs;
- Any person exercising ultimate control over the fund by other means.

In case of foundations, trusts, stichtings etc. the following persons need to be identified in addition to the definition above:

- the settlor;
- any fiduciary or trustee;
- the protector, if any;
- the beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
- any other natural person exercising ultimate control over the fiducial or trust by means of direct or indirect ownership or by other means;

The obligation to identify the beneficial owner and to verify the beneficial owner's identity as provided in Article 3(2)(b) of the Law, shall also include the obligation to take reasonable measures to verify the beneficial owner's identity using relevant information or data obtained from a reliable source such that the professional is satisfied that it knows who the beneficial owner is. If available, the obtained information shall be compared with the information reflected within the national register of Ultimate Beneficial Owners or Register of Fiducies and Trusts.

6 Risk-Based Approach (RBA) and Risk Rating (RiRa)

The RBA is one of the key elements defined in the AML Law article 3 §3 and specified in CSSF 12-02 article 5. It requires the Company to treat every client with a unique and personal risk level, using a scoring model.

The risk rating must be performed upon onboarding and subsequently whenever a material change in a client's risk occurs, or when the regular update cycle requires it. The Company defines the following risk classifications and ongoing review cycles:

Risk Level	Review Cycle
Low Risk	Every four years
Medium Risk	Every two years
High Risk	Annually
Prohibited	Not accepted – at least one factor leads to a breach of legal/regulatory obligations or the Company's risk appetite

As soon as a client is classified as a High Risk Customer (HRC), enhanced due diligence (EDD) is mandatory. Approval by at least one member of Senior Management and the Compliance Officer is required for all HRCs.

Given the nature of the fund as a feeder fund with a single investment in its master fund, the primary counterparties subject to risk assessment are the master fund itself, key service providers, and the limited partners (investors).

7 Politically Exposed Person (PEP)

PEPs represent a sub- category of HRCs. Especially, but not limited to, their enhanced corruption risk, which should be given greater reflection. Depending on the case, special attention might be drawn to certain PEP which are classified as inactive. It can be assumed they may easily use their former status or contacts after their active time has ended. This needs to be assessed on a case by case basis. The general treatment of PEPs is equal to HRCs.

Following the 5th AML Directive the AML law defines a politically exposed person as following:

"Politically exposed persons" (PEPs) shall, in accordance with this law, mean natural persons who are or have been entrusted with prominent public functions and (…) family members or persons known to be close associates, of such persons. (…)

"Natural persons who are or have been entrusted with prominent public functions" shall, in accordance with paragraph 9 above, mean all natural persons, including:

"(a)heads of State, heads of government, ministers and deputy or assistant ministers;

(b)members of parliament "or of similar legislative bodies";

(c)members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;

(d)members of courts of auditors or of the boards "or directorates" of central banks;

(e)ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

(f)members of the administrative, management or supervisory bodies of State-owned enterprises;

(g)important officials "and members of the governing bodies" of political parties;" (Law of 13 February 2018)

(h)directors, deputy directors and members of the board or equivalent function of an international organisation"; (Law of 25 March 2020)

(i)the natural persons exercising the functions included in the list published by the European Commission based on Article 20a(3) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, hereinafter referred to as "Directive (EU) 2015/849. "

None of the categories set out in "(a) to (h)" above shall be understood as covering middle ranking or more junior officials. (…)

(Law of 27 October 2010) "(…) Family members" shall, in accordance with paragraph 9, mean all physical persons, including in particular:

"(a) the spouse;

(b) any partner considered by national law as equivalent to the spouse;

(c) the children and their spouses, or partners "considered by national law as equivalent to a spouse";

(d) the parents;

(e) the brothers and sisters. "

"Persons known to be close associates" shall, in accordance with paragraph 9 above, mean all natural persons, including:

"(a)any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in paragraph 10;

(b)any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in paragraph 10."

Examples of closely related persons to PEPs

- members of the family: siblings (including in-law), nephews and nieces, uncles and aunts, cousins;
- personal assistants or other close persons to the relevant SCC;
- business partners;
- companies, shareholdings, stakes, etc. of a SCC or connected person, where they are ultimate beneficial owners (UBO) as defined in article 23 CSSF 12-02.

Further to PEPs, there are several other special category client types, which require enhanced due diligence due to higher corruption and/or money laundering risk, amongst others:

- charity organizations, not-for-profit organizations (NPOs), non-governmental organizations (NGOs).
- state or government owned enterprises or institutions;
- persons with power of attorney at the highest level for the named artificial persons or bodies or who are UBOs or could exert major influence on these;
- companies with bearer shares or equal structures, where the UBO is not (clearly) known;
- other persons who impose a special risk to the company: e.g. high-ranking dignitaries (Pope, Cardinal, Bishop, etc.), film- and sports-stars, artists, musicians, etc.;
- any client subject to a SAR which has been validated by the FIU (CSSF 12-02 article 48.3).

8 ML Risk Appetite

The declared aim of the Company is not to be involved in any money laundering and/or terrorist financing matters. In consequence, the Company will not:

- Accept assets that are known or suspected to be the proceeds of criminal activity;
- Engage in relationships, directly or indirectly, with terrorists, criminals or their financiers;
- Engage in relationships with Shell Banks or credit institutions known to allow their accounts to be used by a Shell Bank;
- Engage in relationships with persons who use anonymous accounts or accounts with fictitious names;
- Engage in relationships with sanctioned persons or entities as defined by Luxembourg laws, rules and regulations;
- Manage or administer products/funds suspected of being used for money laundering or terrorist financing.

The following principles shall apply:

Investors (Well-Informed Investors):

- Lok Capital V Lux Feeder SCSp targets well-informed investors only as defined under Luxembourg law (institutional investors, professional investors, or investors who have declared themselves well-informed and meet the applicable investment or assessment thresholds). No retail investors shall be accepted.
- Investors registered in high-risk countries (as per the Company's AML Country Risk List) shall only be accepted after enhanced due diligence and with the approval of the Compliance Officer and at least one member of Senior Management.
- High Risk Investors shall be approved by the Compliance Officer and at least one member of Senior Management, after enhanced due diligence.
- Investors who are natural or legal persons, as well as their beneficial owners, for which relevant tax indicators as per CSSF 17/650 (as amended) have been identified shall be approved by at least one member of Senior Management.

Fund and Investment Strategy:

- Lok Capital V Lux Feeder SCSp is a feeder fund structured as a Luxembourg SCSp. Its sole investment is a participation in its master fund. The master fund and its management must be subject to appropriate AML/KYC due diligence.
- No funds/asset strategy with relation to drugs, gambling, cluster munitions, weapons, or cryptocurrency shall be accepted.

Master Fund / Delegates and Service Partners:

- The master fund and any portfolio management delegate must be a regulated investment manager subject to equivalent AML/CTF standards.
- No delegation of Risk Management.
- No High Risk Delegates. Exemption only with Board of Managers Approval.

Russia and Belarus:

- The Company does not intend to accept new business in Russia or Belarus, or with economic Russian or Belarus connection. This concerns contracts with new business partners, investors and assets. Exceptional approval of the Board of Managers is required for any such case.

In case of any doubt or suspicion with respect to unusual transactions, service partners, assets, investors or any other potential ML/TF incident, the Compliance Officer must be informed immediately.

The ML risk appetite of the Company is considered as **medium-low**.

9 TF Risk Appetite

The Company does not intend to take any significant risk concerning Terrorist Financing (TF). The Company will ensure that none of its customers, service partners, assets, investors or related parties are part of any sanctions list of the United Nations or European Union. In case of single cases which are exposed to TF higher risk indicators, enhanced due diligence must be carried out.

The Company prohibits any transaction involving sanctioned entities (UN, EU), anonymous payments, or transactions linked to terrorism. Transactions involving high-risk countries as per the Company's own country risk list shall only be carried out after enhanced due diligence and where clear business justification exists.

The TF risk appetite of the Company is considered as **low**.

10 Responsibility and Accountability

The Compliance Officer (CO) is responsible for the supervision of all policies, procedures and processes at the Company, particularly for AML/CTF and KYC issues. The CO assists the Company and all staff members in achieving compliance with local laws, regulations, circulars and standard market practices, and ensures that employees are informed of regulatory changes and regularly (at least annually) trained in these matters.

The CO is also responsible for communications and cooperation with the supervisory and judicial authorities, and for decision-making within the Company as to whether and when suspicious transactions or activities are to be notified to the state prosecutor (FIU).

In accordance with CSSF 12/552, compliance is a matter for all employees of an institution. All such persons shall take all reasonable steps to avoid money laundering/terrorist financing and remain alert to suspicious issues and Red Flags.

Regarding the AML/KYC obligations of Lok Capital V Lux Feeder SCSp, the board of managers and the designated RR will have the final responsibility for AML/KYC issues.

11 Terrorist Financing Risk

In general, there are three stages of terrorist financing: raising of funds (through either illicit or licit activities); moving the funds; and using the funds. This includes not only the direct financing of acts of terrorism, but also propaganda, recruitment, training, travel and daily operational needs.

The risk of terrorism and terrorist financing is classified as medium as per the sub-sector risk assessment (collective investment sector). Risk-increasing indicators specific to the Company's business model are limited:

- Traditional banking products (debit/credit cards, wire transfers, ATM withdrawals): not offered by the Company.
- NPOs carrying out development and humanitarian projects: any such investors are closely monitored.
- Crowd funding: not served by the Company.
- Frequent cash transactions: not part of the Company's business model.

The Company does not perform cash transactions and does not participate in any crowd funding campaigns. Risk indicators involving NPOs shall be identified through monitoring measures (e.g. KPIs) and assessed as necessary.

12 Proliferation Financing Risk

Proliferation financing risk has increased across the financial industry. In June 2021, FATF published guidance on proliferation financing risk assessment and mitigation. Private sector entities are required to assess, understand and mitigate their proliferation risk within the framework of their existing targeted financial sanctions and compliance programs.

All assets of the fund under management are assessed in the context of a Know Your Asset (KYA) process to identify all key persons and KYA/KYC risks. The Company screens on a daily basis its service partners, key persons, investors, connected persons and all fund assets against sanctions lists and adverse media. Accordingly, any concrete risk of a breach against proliferation financing would be detected within the scope of such screening.

The Company excludes business relationships with shell banks, dummy accounts or other fraudulent intermediaries. The risk of evasion of targeted financial sanctions is considered low.

Furthermore, the Company does not target industries and sectors with specifically increased proliferation risk (armed industry, chemistry, transports, etc.). In case of single assets, investors or service providers with a specific connection to increased risk such as dual-use items, enhanced due diligence must be carried out.

Compliance with the Law implementing the Convention on Cluster Munitions of 4 June 2009 must be ensured at all times. This law prohibits the development, manufacture, assembly, acquisition, sale, use, detention, transport, transfer, stockpiling or retention of cluster munitions or explosive sub-ammunitions (Article 2), and prohibits financing the production of such weapons (Article 3).

13 Dual Use Items

Commission Recommendation (EU) 2024/214 provides guidelines for data gathering and processing for the EU's annual report on controlling dual-use items (goods, software and technology with both civilian and military uses) under Regulation (EU) 2021/821.

Dual Use Items are defined as items, including software and technology, which can be used for both civil and military purposes, and includes items which can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery.

The Company does not serve any funds which mainly target such industries or which directly invest in dual-use items. However, it is possible that Lok Capital V Lux Feeder SCSp may in exceptional circumstances hold indirect exposure through its master fund investment. In such cases, enhanced due diligence is required.

14 Procedure & Process Instruction Regarding AML, CTF and KYC

14.1 Enactment of AML/CTF/KYC Policy

This AML/CTF/KYC Policy aims to enable the Company to be compliant with all applicable local laws, regulations, circulars and standard market practices on the prevention of money laundering and terrorist financing. It is approved by the Board of Managers and is applicable to all employees of the Company.

14.2 Adequate Internal Organisation and Audit

The Company has set up internal control and communication procedures and structures which adequately prevent money laundering transactions and activity. This comprises the nomination of a designated member of the Board of Directors responsible for Compliance and AML/CTF, the nomination of a CO responsible for AML/CTF and Compliance, and the establishment of relevant policies, procedures and processes which must be strictly adhered to. Any non-compliance may be penalized according to the Code of Conduct.

14.3 Know-Your-Customer (KYC), Know-Your-Delegate/Counterparty

The local laws, regulations, circulars and standard market practices give a clear and precise definition of the steps to be undertaken to conduct a proper KYC. These steps are applicable to any business, professional or commercial relationship which is intended to be for a certain period of time.

The Company will not open numbered or anonymous accounts or accept client relationships where the ultimate beneficial owner of invested assets cannot be determined.

In its function as a registered AIFM and GP, the Company can delegate part or all of its AML/KYC duties to delegates. Any delegate or counterparty shall only be accepted if it has previously contractually imposed equivalent identification and monitoring requirements. The ultimate responsibility for AML/CTF/KYC obligations always rests with the Company.

The Company does not currently and will not work with or accept business from shell banks of any jurisdiction.

15 Client Acceptance Process (CAP)

The CAP was shaped around the AML Law and CSSF 12-02 (especially article 5) to cover the following key aspects:

- Identification and verification of clients (including the master fund, investors, service providers), their signatories/proxy holders and/or UBOs;
- Risk-based classification of any client using a scoring model;
- Ongoing monitoring of clients and regular updates of relevant data according to their level of risk.

Given the feeder fund structure, the primary KYC focus areas are:

- The master fund and its AIFM/GP: full KYC including AML/CTF framework verification, regulatory status, UBO identification and risk assessment;
- Well-informed investors (limited partners): identification, verification, source of funds, source of wealth, UBO identification and risk rating;
- Key service providers (administrator, auditor, legal counsel, custodian etc.): KYC proportionate to delegated functions and associated risk.

Every new client relationship must be assessed on a four-eyes principle. New client relationships must also be approved by at least one member of Senior Management. In case of disagreement or a high risk classification, the Senior Management shall decide collectively.

Adverse media analysis is to be performed on prospect clients before establishing a business relationship, and on a regular basis thereafter to detect and anticipate risk.

All refused or terminated clients due to ML reasons will be recorded in a dedicated register and, if applicable, a SAR may be filed by the CO.

The Compliance department will maintain a database of all onboarded customers and their related parties (e.g. UBOs, representatives), subject to regular (daily) sanctions and PEP screening via an automated screening tool.

16 Know Your Colleagues / Staff

As required by Article 45 of CSSF 12-02, the Company implements processes for hiring staff which include checks on appropriate honesty, experience and skills. All members of the Board must provide an extract from the police records or comparable documentation.

All staff members, regardless of position or seniority, will be regularly (at least once a year) subject to sanction screenings.

17 Ongoing Monitoring of Clients / Sanction Screening

After the initial screening, all clients, related persons, investments and other relevant parties/persons including their UBOs are screened on a daily basis using an automated sanction screening tool (e.g. LSEG WorldCheck or equivalent).

All clients are subject to periodical screening against official sanctions and PEP lists, as required by the AML Law and CSSF 12-02 article 33.1. The data is checked against watch lists and potential list matches, creating alerts in the case management system.

Alerts must be analysed and assessed by members of the Compliance team within 1 business day, handled by a minimum of 2 team members. In case of a true match with an EU or UN sanctioned entity, the RC must be informed immediately. Any positive EU or UN sanctions match must be reported to the Ministry of Finance without delay.

When adverse media elements are discovered as part of the ongoing due diligence, a compliance opinion must be produced for all true positives and escalated to the Board of Managers of the Company.

For existing customers identified as PEPs through daily screening, completion of the due diligence and approval to continue the relationship must take place within 1 month of the detection of the PEP status.

18 Monitoring and Recognition of Suspicious Transactions and Activities

It is the Company's responsibility to ensure the monitoring of transactions and activities to be able to fully cooperate with the authorities, independent of whether it has delegated any identification act and ongoing monitoring to a third party.

Special care will be taken when operating transactions or facing activity at the following levels:

- Difficulties in obtaining identification documents;
- Contradicting or inconsistent information provided by any client, investor, delegate or counterparty;
- Frequent address changes;
- Provision of a PO Box address only;
- Frequent changes in payment details;
- Incomplete application details or lack of willingness to provide required evidence;
- Any transaction or activity connected to HRCs or SCCs;
- Any transaction or activity related to High-Risk Countries;
- Any unexpected or implausible transactions or activities, including:
  - In-out transactions for substantial amounts on a short-term basis;
  - Disproportionate transaction volumes compared to usual transactions;
  - Activation of dormant accounts;
  - Payment of redemption proceeds to a third-party account unconnected to the investor's account;
  - Several transfers from different individual accounts to one investor's account;
  - Frequent and large transfers arriving from different countries;
  - Asset transfers to/from countries unrelated to the investor's residence.

The above list is illustrative and not exhaustive.

Where any suspicious transaction or activity is identified, the Company will immediately file a SAR to the FIU, or in case of sanction hits to the Ministry of Finance and the CSSF, whenever the CO autonomously considers that the suspicion is to be escalated.

19 Cooperation with the Authorities

In accordance with AML Law article 5 and CSSF 12-02 articles 47 & 48, the Company, its Board of Directors, Senior Management and all staff are obliged to fully cooperate with the Luxembourg authorities responsible for combating money laundering and terrorist financing. This includes:

- Informing, without delay and on their own initiative, the FIU when they know, suspect or have reasonable grounds to suspect that money laundering is being or has been committed or attempted (SAR);
- Providing, without delay and upon request, any information and documents to the FIU;
- Refraining from carrying out any transaction or activity which is known or suspected to be related to money laundering or terrorist financing before having informed the FIU;
- Complying with any instruction from the FIU to block the execution of one or more operations (maximum 3 months, extendable to a maximum of 6 months in writing).

Good faith disclosure to the Luxembourg authorities responsible for combating money laundering and terrorist financing does not constitute a breach of any restriction on disclosure of information and shall not involve the disclosing persons in any liability.

20 No Tipping Off

In accordance with AML Law article 5 §5, the Company and all its employees shall not disclose to the customer concerned or to any third person the fact that information has been reported to the authorities, or that a money laundering or terrorist financing investigation by the FIU is being or may be carried out. This prohibition does not apply to disclosures to competent authorities or self-regulatory bodies.

21 Data Protection

Personal data of a customer collected by the Company during the business relationship and/or an occasional transaction shall be deleted at the end of the five (5) year retention period following the end of such business relationship/occasional transaction.

In accordance with Article 1(5) of the Grand-ducal Regulation of 1 February 2010, each individual transaction record must contain: the name of the customer and beneficiary; address or other identifying information; nature and date of the transaction; type and amount of currency involved; and the type and identifying number of any account involved.

By way of derogation, the personal data may be retained for an additional five (5) years where this is necessary to effectively implement internal measures for the prevention or detection of money laundering or terrorist financing (Article 3(6) AML Law).

Personal data shall be processed only for the purposes of the prevention of money laundering and terrorist financing and shall not be further processed in a way incompatible with those purposes (Article 3(6a) AML Law).

22 Sanctions for Breach of Professional Obligations

The intentional breach of professional obligations relating to the fight against money laundering and terrorist financing is a criminal offence and a fine of between EUR 1,250 and EUR 1,250,000 may be imposed on any person knowingly contravening the applicable laws. The CSSF is also empowered to impose sanctions.

Company-internal sanctions for employees on non-observance of the applicable laws will be determined by the Board of Directors on a case-by-case basis, including but not necessarily limited to dismissal.

23 Regular General Risk Analysis on AML & CTF and Yearly Reports

In accordance with CSSF Circular 11/529, the CO is obliged to regularly (at least yearly) conduct a risk analysis concerning the AML/CTF risk to which the Company is exposed. The risk analysis must comprise major changes in client structure, new products or major changes to existing products, changes to the Company's AML Country Risk List, and any other developments which may change the Company's AML/CTF risk profile.

Based on the results of the risk analysis, the CO will provide a report to the Board of Managers (CSSF 12-02 article 42 §6). This report will also form part of the annual Compliance report to be provided to the Board of Managers and the CSSF (at the latest one month after the yearly general assembly has taken place).

24 Ongoing Training and Awareness Programme

The Company has implemented measures to train all staff and raise awareness on money laundering matters on an ongoing basis. The training programme covers all members of staff, including management body members and authorised management.

The CO ensures that at least yearly AML training is organised, covering Luxembourg-specific AML and TF topics relevant to the fund industry. This training is mandatory for all employees. Board members may alternatively participate in adequate external training, provided proof of participation is submitted within the year.

Newly hired employees will be informed about the Company's policies and procedures not later than one month after the beginning of their working contract. A basic AML and KYC training shall be offered to each newly hired employee to ensure foundational knowledge of AML and KYC processes.

25 Distribution of this AML- Policy

This policy is accessible to all employees to help them meet their obligations regarding AML/CTF and KYC by defining clear and precise procedures and processes. The latter should be adhered to at all times and always in the spirit and the wording of the relevant laws, regulations, circulars and standard market practices. The AML-Policy is not foreseen for distribution with external parties. However, exemptions can be made for auditors or financial supervisory authorities for instance.

Approval

This AIF-specific AML Policy has been adopted by the Board of Managers of LCV Lux GP S.a r.l. on the date indicated in the Version History above.

Jens Mühlenfeld | Manager

Signature: Jens Mühlenfeld ______________________

Date: 11.08.2026

Saari El-Kurd | Manager

Signature: ______________________

Date: 11.08.2026

Ingo Prummenbaum | Manager

Signature: ______________________

Date: 11.08.2026

Benedikt Gansen | Responsable du Contrôle (RC)

Signature: ______________________

Date: 11.08.2026