Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

Anti-Money Laundering and Counter Terrorist Financing Compliance Policy

Web3 Solutions S.r.l

Via del Lauro 9, 20121, Milan, Italy

Version: 1.1
Date: December 2024
Document ID: ITW-01

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

Version	Completed by	Approved by
1.1	Akshatha Arjun Babu Naidu MLRO	Roman Rashimas Director
		

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

Contents

1. Introduction 7
1.1 Web3 and its Services 7
1.2 Authority & Scope of the AML/CTF Policy 7
1.2.1 Define Roles and Responsibilities 8
1.2.2 Risk Assessment Process 8
1.2.3 Internal Control Framework 8
1.2.4 Know Your Customer (KYC) Framework 9
1.2.5 Transaction Monitoring and Reporting 9
1.2.6 Sanctions Compliance 9
1.2.7 Recordkeeping and Documentation 9
1.2.8 Training Programme 9
1.2.9 Independent Testing and Auditing 9
1.2.10 Accountability of the Board 9
1.2.11 Risk-Based Approach 10
1.2.12 Independent AML/CTF Function 10
1.2.13 Review of the Policy 10
1.3 AML/CTF Legal Framework 10
1.3.11 Nullification of Non-Compliant Provisions 10
1.3.12 Modification of Policy Provisions 11
1.3.13 Avoidance of Non-Compliant Actions 11
1.4 The Italy and Italian law and regulation 11
2. Overview of MiCAR and Its Regulatory Requirements in Italy 12
1.5 Regulatory Requirements 12
2.1.1 Timeline for Implementation 13
2.1.2 Regulation of Issuers of Crypto-Assets Other Than EMTs & ARTs 13
2.1.3 Regulation of Issuers of ARTs & EMTs (are we dealing with ARTs and EMTs???) 14
3. Definitions 15

Version: 1.1
Date: December 2024
Document ID: ITW-01

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

4. Roles and Responsibilities 19
5. Comprehensive Measures Implemented by Web3 Solutions to Prevent Money Laundering and Terrorist Financing 22
6. Company's Structure 30
6.1 Parent Company: Lunu Solutions GmbH 30
6.2 Subsidiary: Web3 Solutions S.r.l 30
6.3 Names of the managers and members of the Board of Directors 30
7. BUSINESS WIDE ML / TF RISK ASSESSMENT 31
8. Internal Control Procedures 32
9. Customer Risk Scoring 33
9.5 Customer Due Diligence 34
10. Identification of The Customer and The Beneficial Owner 40
11. Risk factors 41
11.1 Prohibited Customers 43
11.2 Customer Screening 44
12. Reporting Suspicious Activities and Cooperating with Authorities 45
13. AML/CTF Training 46
14. Abandoned and Dormant Accounts 47
15. Record Keeping 47
16. Oversight and Responsibility 49
Appendix 1. Country Risk Matrix 49
Appendix 2. Customer Identification and Verification 50
Appendix 3. Retailer or Customer Risk Matrix 52
Appendix 4. High Risk and Prohibited Industries 53

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

List of Abbreviations

AEC	Anonymized Cryptocurrency
AML	Anti-Money Laundering
AMLD5	Anti-Money Laundering Directive5
ARTs	Asset-Referenced Tokens
CASPs	Crypto Asset Service Providers
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CTF	Counter-Terrorism Financing
DNS	Domain Name System
EDD	Enhanced Due Diligence
EMTs	Electronic Money Tokens
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
ICO	Initial Coin Offering
ID	Identification
IP	Internet Protocol
JADIS	Joint Anti-Money Laundering and Terrorist Financing Information System
KYB	Know Your Business
KYC	Know Your Customer
KYT	Know Your Transaction
MiCA	Markets in Crypto-Assets
MiCAR	Markets in Crypto-Assets Regulation
ML	Money Laundering
MLRO	Money Laundering Reporting
ODD	Ongoing Due Diligence
OFAC	Office of Foreign Assets Control
P2P	Peer-to-Peer
PEP	politically exposed person
POS	point-of-sale
SAR	Suspicious Activity Reporting
SDD	Simplified Due diligence
STR	Suspicious Transaction Reporting
TF	Terrorist Financing
TIN	Tax Identification Number
UBO	Ultimate Beneficial Owner
UIF	Unità di Informazione Finanziaria
VA	Virtual Asset
VASP	Virtual Asset Service Provider

Version: 1.1
Date: December 2024
Document ID: ITW-01

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

1. Introduction

1.1 Web3 and its Services

Web3 Solutions S.r.l (hereinafter collectively referred to as "we," "us," "Web3"), is a Virtual Asset Service Provider (VASP) offering cryptocurrency payment solutions, enabling Retailers to accept payments in cryptocurrencies. Web3 Solutions S.r.l is regulated in Italy under Legislative Act no. 90, which includes cryptocurrencies and blockchain within the legislative framework. The decree, enacted in 2017, aligns cryptocurrency exchanges with foreign currency exchanges, though it clarifies that cryptocurrencies are not issued by a central bank and are not linked to traditional currencies, but serve as a virtual medium of exchange for goods and services.

Web3 Solutions S.r.l is subject to Italy's updated Anti-Money Laundering (AML) regulations, specifically designed for crypto firms, which were published in February 2022. These regulations are part of a broader effort to enhance the oversight and transparency of virtual asset service providers (VASPs) and to combat illicit activities such as money laundering and terrorist financing in the digital asset space. Our AML rules for crypto firms in Italy align with the European Union's Fifth Anti-Money Laundering Directive (AMLD5) which requires VASPs to comply with stringent anti-money laundering standards. Additionally, the rules reflect the Financial Action Task Force (FATF) guidelines, an international standard for combating financial crime, ensuring that VASPs in Italy operate under comprehensive reporting and compliance obligations.

Additionally, Web3 Solutions S.r.l operates in the European market under the Markets in Crypto-Assets Regulation (MiCAR), established through Regulation (EU) 2023/1114. This regulation, officially enacted on June 29, 2023, provides a harmonized framework across the EU for issuing crypto-assets and offering related services. MiCAR aims to address regulatory gaps, ensuring transparency, market integrity, and the proper oversight of crypto-asset markets.

The primary revenue streams for Web3 Solutions S.r.l include fees paid by Retailers for payment services, as well as the sale of point-of-sale (POS) terminals. Web3 Solutions S.r.l is committed to full compliance with Italian and EU AML regulations to prevent money laundering and terrorist financing in the cryptocurrency sector.

1.2 Authority & Scope of the AML/CTF Policy

The Anti-Money Laundering ("AML") and Counter-Terrorism Financing ("CTF") Policy (hereinafter referred to as the "Policy") is issued under the authority of Web3 Solutions S.r.l's Board of Directors (the "Board"). This Policy applies to all employees, staff, officers, and directors of Web3 Solutions S.r.l, including its

associated entities. The provisions of this Policy, along with any future amendments or additions, are incorporated into and form part of the terms and conditions of employment for all employees in accordance with their contracts.

This Policy establishes the compliance framework that Web3 Solutions S.r.l will use to ensure adherence to all applicable AML/CTF laws and regulations within Italy and the European Union. The Policy is intended to guide the Board, employees, staff, officers, and directors in conducting Web3's business in full compliance with these laws. Web3 Solutions S.r.l has developed its products and services with a strong focus on compliance and security to prevent their use for illegal or illicit purposes. The company is committed to maintaining the highest possible level of compliance with all relevant AML/CTF legislation and regulations.

All employees, staff, officers, and directors of Web3 Solutions S.r.l are required to participate in annual compliance training programs to reinforce Web3's commitment to a compliance-driven culture. These training programs ensure that everyone at Web3 is informed of their responsibilities under the AML/CTF laws and understands how to act in accordance with this Policy. The company will maintain rigorous AML/CTF controls at all times in accordance with applicable laws, with a zero-tolerance approach towards non-compliance. The policy intends to stick to the following guidelines:

1.2.1 Define Roles and Responsibilities

Clearly outline the roles and responsibilities of Web3 Solutions S.r.l's AML/CTF compliance personnel, including the Money Laundering Reporting Officer (MLRO) and other relevant officers, to ensure accountability in managing the company's compliance obligations. The responsibility for adhering to this Policy extends to all employees, staff, officers, and directors, including full-time, temporary, part-time employees, interns, and contractors. This includes individuals directly or indirectly facing customers, those responsible for executing or overseeing transactions, managing contractual documentation, maintaining systems and tools, or handling any other sources of information that could reveal indications of potential money laundering or terrorist financing. All such personnel must be fully familiar with this Policy as it pertains to their specific responsibilities and are expected to act in strict accordance with its provisions.

1.2.2 Risk Assessment Process

Shall establish a comprehensive risk assessment process to identify, assess, and mitigate the potential risks associated with money laundering and terrorist financing. This includes evaluating customer profiles, transactions, and business activities in line with risk-based methodologies.

1.2.3 Internal Control Framework

Shall outline Web3 Solutions S.r.l's internal controls for AML/CTF compliance. This encompasses policies, procedures, and controls to prevent, detect, and report suspicious activities and ensure adherence to all relevant laws and regulations.

1.2.4 Know Your Customer (KYC) Framework

Develop and implement a robust KYC framework that includes customer identification, verification, and due diligence processes. These processes will be risk-based, ensuring that higher-risk customers and transactions receive enhanced scrutiny, in line with Italy's regulatory requirements and MiCAR provisions.

1.2.5 Transaction Monitoring and Reporting

Shall establish a transaction monitoring system to detect and flag unusual or suspicious transactions. This system will be complemented by a Suspicious Activity Reporting (SAR) programme that ensures timely and accurate reporting of any potentially illicit activities to the appropriate authorities, including the Financial Intelligence Unit (FIU).

1.2.6 Sanctions Compliance

Implement controls to ensure compliance with international sanctions regimes. This includes regular screening of customers, transactions, and counterparties against official public financial sanctions lists, such as those maintained by the European Union, United Nations, and other relevant bodies.

1.2.7 Recordkeeping and Documentation

Ensure that Web3 Solutions S.r.l properly documents all efforts to comply with legal and regulatory requirements, including maintaining records in accordance with Italian and EU regulations, as well as MiCAR's reporting and record-keeping standards.

1.2.8 Training Programme

Provide comprehensive AML/CTF training for all employees, staff, officers, and directors of Web3 Solutions S.r.l. The training programme will be designed to ensure that everyone in the company understands their role in AML/CTF compliance and remains informed about current regulatory requirements, risks, and best practices.

1.2.9 Independent Testing and Auditing

Perform periodic independent testing of Web3 Solutions S.r.l's AML/CTF programme, ensuring that Web3's compliance controls remain effective, are regularly updated, and are adapted to address any weaknesses or emerging risks.

1.2.10 Accountability of the Board

The Board of Web3 Solutions S.r.l holds ultimate responsibility for approving this Policy and ensuring its proper implementation. The Board is tasked with promoting a culture of compliance within Web3, ensuring that all employees and stakeholders prioritize adherence to AML/CTF laws and regulations.

1.2.11 Risk-Based Approach

Web3 Solutions S.r.l has adopted a risk-based approach to mitigate the risk of being exploited for money laundering or terrorist financing. The rules, requirements, and procedures outlined in this Policy must be followed at all times. In cases of non-compliance, Web3 Solutions S.r.l reserves the right to take disciplinary action, up to and including dismissal, for employees, staff, officers, or directors who fail to comply.

1.2.12 Independent AML/CTF Function

The AML/CTF function at Web3 Solutions S.r.l is an independent function led and managed by the company's Money Laundering Reporting Officer ("MLRO"). The MLRO is responsible for regularly updating the Board of Directors on all material issues related to the AML/CTF program. The AML/CTF program includes, but is not limited to, the following core activities:

1. Customer identification processes (Know Your Customer - KYC)
2. Defining eligible and non-eligible activities
3. Sanctions screening
4. Transactional monitoring
5. Regular risk assessments
6. Reporting of suspicious activities
7. Record-keeping procedures
8. Employee training programs
9. Other pertinent compliance activities required by applicable AML/CTF laws

1.2.13 Review of the Policy

This Policy will be reviewed by Web3 Solutions S.r.l at least once every year to ensure that it remains up-to-date with the latest legal, regulatory, and industry developments in Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF). The review process will ensure the Policy reflects any newly enacted or amended regulations that impact the company's operations, both at a national and international level.

1.3 AML/CTF Legal Framework

Web3 Solutions S.r.l will comply with all applicable laws, regulations, rules, directives, orders, and requirements related to Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) (hereinafter referred to as "AML/CTF applicable laws"). These include, but are not limited to, the specific obligations outlined in Section 1.5 of this Policy.

In the event that any provision of this Policy leads, directly or indirectly, to non-compliance by Web3 Solutions S.r.l or its employees, staff, officers, and directors with any AML/CTF applicable laws, the following actions will be taken:

1.3.11 Nullification of Non-Compliant Provisions

Any provision of this Policy that causes Web3 Solutions S.r.l or its employees, staff, officers, and directors to be in non-compliance with AML/CTF applicable laws will be deemed null and void, but only to the extent

necessary to eliminate the non-compliance. This ensures that the Policy remains in full compliance with all applicable legal and regulatory requirements.

1.3.12 Modification of Policy Provisions

Web3 Solutions S.r.l, along with its employees, staff, officers, and directors, will take the necessary steps to amend, supplement, or modify the relevant provisions of this Policy. Such adjustments will be made to ensure that Web3 Solutions S.r.l remains in full compliance with the AML/CTF applicable laws at all times. This may involve revising procedures, implementing new controls, or introducing additional measures to rectify any non-compliant aspects of the Policy.

1.3.13 Avoidance of Non-Compliant Actions

Web3 Solutions S.r.l and its employees, staff, officers, and directors shall also have the right to refrain from taking any actions that would result in continued or future non-compliance with AML/CTF applicable laws. This ensures that all actions taken by the company and its personnel are fully compliant and legally sound.

1.4 The Italy and Italian law and regulation

The AML/CTF applicable laws in Italy, with which Web3 Solutions S.r.l and its employees, staff, officers, and directors must comply, include but strictly are not limited to the following:

1. **Italian Legislative Decree No. 231/2007 (as amended):** This legislative decree implements the European Union's anti-money laundering directives, including AMLD5, into Italian law. It establishes requirements for customer due diligence, record-keeping, and reporting suspicious activities related to money laundering and terrorist financing.
2. **Regulation (EU) 2015/847 on Information Accompanying Transfers of Funds**: This EU regulation requires that specific information regarding the payer and payee be included in fund transfers. Web3 Solutions S.r.l must ensure compliance with these rules to prevent the misuse of funds for illicit purposes, such as money laundering and terrorist financing.
3. **MiCAR (Markets in Crypto-Assets Regulation) – Regulation (EU) 2023/1114:** As a Virtual Asset Service Provider (VASP) under MiCAR, Web3 Solutions S.r.l must adhere to this new regulation, which provides a comprehensive framework for the issuance and offering of crypto-assets and related services across the European Union. It ensures consistency in the approach to the crypto market, covering transparency, governance, and consumer protection standards, while also addressing risks linked to money laundering and terrorism financing.
4. **Financial Action Task Force (FATF) Recommendations:** Italy, as a member of the FATF, adheres to international AML/CTF standards established by this body. Web3 Solutions S.r.l is obligated to comply with these recommendations, which provide the foundational principles for combating money laundering and terrorism financing on a global scale.
5. **Italian Central Bank and Consob Guidelines:** Web3 Solutions S.r.l must also follow the specific guidelines issued by Italy's financial authorities, including the Bank of Italy and Consob (Commissione Nazionale per le Società e la Borsa), which regulate aspects of financial transactions, anti-money laundering procedures, and oversight of virtual assets in the country.

6. **EU Fifth Anti-Money Laundering Directive (AMLD5):** As an Italian VASP, Web3 Solutions S.r.l must ensure compliance with AMLD5, which includes provisions for enhanced due diligence, reporting obligations, and customer verification processes. The directive aims to combat the financing of terrorism and reduce risks associated with money laundering in the financial sector.
7. **Italian Data Protection Regulations (GDPR):** Ensuring that customer data is handled in compliance with the General Data Protection Regulation (GDPR) is crucial in implementing AML/CTF practices. Web3 Solutions S.r.l is committed to protecting personal data in accordance with Italian and EU data protection laws while also fulfilling its AML/CTF obligations.

2. Overview of MiCAR and Its Regulatory Requirements in Italy

1.5 Regulatory Requirements

The Markets in Crypto-Assets Regulation (Regulation (EU) 2023/1114) (MiCA) officially came into force in June 2023. Its primary objective is to harmonize the regulatory framework for crypto-assets that are not covered by existing financial services legislation across the European Union. By establishing a unified set of rules, MiCA aims to enhance market integrity and promote financial stability in the crypto-asset sector.

MiCAR provides a comprehensive regulatory framework for crypto-assets within the European Union, categorizing them into three main types, each with distinct characteristics and regulatory requirements. Here's a detailed breakdown:

1. **Electronic Money Tokens (EMTs):** These tokens are designed to maintain a stable value by being directly linked to the value of a single official currency, such as the euro. EMTs function similarly to electronic money, providing a digital alternative to fiat currency.
2. **Asset-Referenced Tokens (ARTs):** ARTs are intended to stabilize their value by referencing a combination of assets, rights, or one or more official currencies. These tokens could be linked to commodities, securities, or other forms of assets, making them versatile in terms of their underlying value reference.
3. **Other Crypto-Assets:** This category encompasses all other types of crypto-assets that do not fall under the definitions of EMTs or ARTs. It includes a broad range of digital assets, such as utility tokens, that are not intended to serve as a means of payment or store of value.

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

2.1.1 Timeline for Implementation

The full application of MiCAR is scheduled for December 30, 2024. However, specific provisions concerning EMTs and ARTs, particularly those related to their issuance, public offering, and admission to trading, will come into force earlier, on June 30, 2024. From these dates, only entities expressly authorized under MiCAR will be permitted to issue or offer ARTs and EMTs to the public or seek their admission to trading.

2.1.2 Regulation of Issuers of Crypto-Assets Other Than EMTs & ARTs

Under the MiCAR, the offering to the public within the EU of crypto-assets that do not constitute EMTs or ARTs or their admission to trading on a trading platform for crypto-assets is subject to the following main requirements:

1. The public issuance of a white paper in accordance with content and form requirements set out in MiCAR and its notification to supervisory authorities.
2. conduct regulation requirements as well as additional obligations regarding commercial communications.
3. inclusion in the white papers of information on the main adverse effects of the crypto-asset on the climate and the environment.
4. transparency obligations when advertising the public offering or trading of the crypto-asset.
5. obligation of issuers to address the right of retail holders within 14 days to withdraw from holding the crypto-asset.
6. obligations to act honestly, fairly, professionally, act to the best interest of the crypto-asset retail holders, without conflict of interest, and maintain all systems and security access protocols according to appropriate EU standards

2.1.3 Regulation of Issuers of ARTs & EMTs (are we dealing with ARTs and EMTs???)

The public offering of Asset-Referenced Tokens (ARTs) or Electronic Money Tokens (EMTs) in the EU requires prior authorization from the national supervisory authorities of the issuer's registered seat,

granted within three months of application. This authorization is valid across the EU, enabling issuers to offer their tokens or seek admission for trading throughout the Union. Additionally, a white paper that meets MiCAR's requirements must be issued, along with notification to supervisory authorities and publication with other marketing communications.

In addition, issuers of EMTs or ARTs are required to:

1. act in good faith, refrain from misleading practices and, in general, act in the best interest of the crypto-asset retail holders.
2. make their marketing communications identifiable and consistent with the white paper;
3. publish on their website their approved crypto-asset white paper and their marketing communications.
4. disclose on their website, at least every month, the number of tokens in circulation and the value and composition of the reserve assets.
5. address the right of retail holders within 14 days to withdraw from holding the crypto-asset.
6. set up internal complaint handling procedures.
7. set up procedures to prevent, identify and disclose conflicts of interests.
8. notify their competent authorities of any changes to their management body.
9. have robust governance arrangements such as clear organisational structure, competent members in management, business continuity policy etc.
10. refrain from granting interest to retail holders.
11. have in place redemption plans to compensate retail holders, in case of insolvency.

2.1.3 Note: Issuers of Electronic Money Tokens (EMTs) or Asset-Referenced Tokens (ARTs) must adhere to specific prudential requirements. They are required to maintain own funds that are at least equal to the greater of the following:
(i) EUR 350,000
(ii) 2% of the average amount of their reserve assets
(iii) a quarter of the fixed overheads from the preceding year
Additionally, issuers must ensure that their reserve assets are legally and operationally segregated from their own estate and from the reserve assets of other tokens.

Due to the fact that EMTs are considered electronic money within the meaning of the Electronic Money Directive (“EMD”) and fall within its scope, the MiCAR provides for additional obligations for issuers of EMTs, which act as lex specialis vis-à-vis the EMD. In specific, under the MiCAR:

1. issuers must be authorized as electronic money institutions under EMD or as credit institutions.
2. the issuance of EMTs is required to be conducted at par value on the receipt of funds.
3. holders may at any time redeem the value of the EMT in cash or by credit transfer;
4. the redemption of e-money tokens shall not be subject to a fee.
5. funds received in exchange of EMTs shall only be invested in secure, low risk assets or deposited in a separate account of a credit institution. At least 30% of the funds must be deposits.

2.1.4 General Regulation under the MiCAR for all category of CASPs

1. obligation to behave honestly, fairly and professionally in the interest of their clients.
2. obligation to have, at all times, precautionary safeguards equal to an amount of at least the higher of the following:
   - amount of the permanent minimum capital requirements set out by the MiCAR (as in 2.1.3 Note), or
   - one quarter of the previous year's fixed overheads, reviewed annually.

3. disclosure of information on the main adverse effects of crypto-assets on the climate and the environment.
4. establishment of a governance framework, especially in relation to management executives and policies and procedures that ensure the compliance with the Act.
5. obligation for the safe custody of crypto-assets and customer funds.
6. establishment of internal complaint handling procedures.
7. identification, prevention, management and disclosure of conflicts of interest.
8. obligations for the management of outsourcing agreements.
9. redemption plans in case of insolvency.
10. obligations in relation to the acquisition of crypto-asset service providers.

3. Definitions

This Policy is subject of review by the Management Board at least annually. The proposal for a review and the review of this Policy may be scheduled more often by the decision of the Company's Money Laundering Reporting Officer (" MLRO") or the Internal Control Officer.

1. **The Company** means legal entity with following data:
   - company name:"Web3 Solutions S.r.l"
   - registration number: "13774000965"
   - address: "Via del Lauro 9, 20121, Milan, Italy"
   - email: info@lunu.io

2. **The Policy** outlines the Company's internal control standards and risk assessment policy for managing ML/TF risks.

3. **The Money Laundering** ("ML") means the concealment of the origins of illicit funds through their introduction into the legal economic system and transactions that appear to be legitimate.

There are three recognized stages in the money laundering process:

- **placement**, which involves placing the proceeds of crime into the financial system.
- **layering**, which involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

source and ownership of funds.

- **integration**, which involves placing the laundered proceeds back into the economy to create the perception of legitimacy;

4. **Terrorist act**: is defined under the United Nations (Anti-Terrorism) Regulations as:
the use or threat of action —

(*a*)	where the action —	
	(i)	involves serious violence against a person;
	(ii)	involves serious damage to property;
	(iii)	endangers a person's life;
	(iv)	creates a serious risk to the health or the safety of the public or a section of the public;
	(v)	involves the use of firearms or explosives;
	(vi)	involves releasing into the environment or any part thereof, or distributing or otherwise exposing the public or any part thereof to —
		(A) any dangerous, hazardous, radioactive or harmful substance;
		(B) any toxic chemical; or
		(C) any microbial or other biological agent, or toxin;
	(vii)	is designed to disrupt any public computer system or the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure;
	(viii)	is designed to disrupt the provision of essential emergency services such as the police, civil defence and medical services; or
	(ix)	involves prejudice to public security or national defence; and
(*b*)	where the use or threat is intended or reasonably regarded as intending to —	
	(i)	any government; or
	(ii)	intimidate the public or a section of the public.

5. **The Terrorist Financing** (TF) means the financing and supporting of an act of terrorism and commissioning thereof as well as the financing and supporting of travel for the purpose of terrorism in the meaning of applicable legislation.
6. **Virtual currency address** shall mean an address/account generated from letters, numbers and/or symbols in the blockchain, by which the blockchain allocates the virtual currency to the owner or recipient.
7. **Virtual currency exchange operator** shall mean a legal person who is established in the Italy or who is a branch, established in the Italy, of a legal person of a Member State of the European Union or a foreign state and who provides services of virtual currency exchange, purchase and/or

sale for remuneration.

8. **Initial Coin Offering** (ICO) shall mean an offer made for the first time directly or through an intermediary by a legal person established in the Italy or a branch of a legal person of a Member State of the European Union or a foreign state established in the Italy to purchase its virtual currencies for funds or other virtual currencies with a view to raising capital or investment.
9. **Customer** means a natural person or a legal entity which has the Business Relationship with the Company or a natural person or legal entity with which the Company enters into the Occasional Transaction.
10. **Beneficial Owner** means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation, step, or exercises control in another manner over a transaction, act, action, operation, step, or over another person and in whose interests, or for whose benefit, or on whose account a transaction, act, action, operation, or step is made. In the case of a legal entity, the Beneficial Owner is a natural person whose direct or indirect holding, or the sum of all direct and indirect holdings in the person, exceeds 25 percent (%), including holdings in the form of shares or other forms.
11. **Proxy holder** refers to any natural person who has received an appointment on behalf of a member of an organisation to attend a meeting and to exercise the appointer's voting rights at that meeting, where applicable.
12. **Know Your Customer** or KYC means procedures implemented to establish and verify the identity of retailers and customers of Web3 before or during their business relationship with Web3.
13. **Client Due Diligence** or CDD means procedures implemented to verify certain aspects about retailers and customers' identity on an ongoing basis, as well as the identification of a Beneficial Owner of an entity, where applicable.
14. Monetary Operation means any payment, transfer or receipt of money.
15. **Virtual currency** means a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4(25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, pp 35–127) or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same Directive.
16. **Sanctions** mean an essential tool of foreign policy aimed at supporting the maintenance or restoration of peace, international security, democracy, and the rule of law, following human rights and international law or achieving other objectives of the United Nations Charter or the common foreign and security policy of the European Union. Sanctions include:
    1. international Sanctions which are imposed with regard to a state, territory, territorial unit, regime, organization, association, group, or person by a resolution of the United Nations

Security Council, a decision of the Council of the European Union or any other legislation imposing obligations on Italy;

2. Sanctions of the Government of the Italy which is a tool of foreign policy which may be imposed in addition to the objectives specified in previous clause in order to protect the security or interests of Italy.

17. **Virtual Currency Address** means the address/account generated from letters, numbers and/or symbols in the blockchain, by which the blockchain allocates the Virtual Currency to the owner or recipient.
18. **Politically Exposed Person ("PEP")** means a natural person who performs or has performed prominent public functions, and with regard to whom related risks remain. (Currently we are not onboarding any PEPs)

The following individuals are considered Politically Exposed Persons (PEPs):

1. Heads of state or government, ministers, vice-ministers or deputy ministers, secretaries of state, and chancellors of parliament, government, or ministries.
2. Members of parliament.
3. Justices of the Supreme Court, Constitutional Court, or other highest judicial authorities whose decisions are final.
4. Mayors and heads of municipal administrations.
5. Members of management bodies of top state audit or control institutions, chairs, deputy chairs, or board members of the central bank.
6. Ambassadors, chargés d'affaires, heads of the armed forces, commanders, chiefs of defense staff, and senior officers of foreign armed forces.
7. Members of the management or supervisory bodies of public or private companies with more than half of their shares owned by the state.
8. Members of the management or supervisory bodies of municipal enterprises or large public or private companies, with significant state ownership, classified as large enterprises under the Law on Financial Statements of Entities of Italy.
9. Directors, deputy directors, or members of the management or supervisory bodies of international intergovernmental organizations.
10. Leaders, deputy leaders, or members of the management bodies of political parties.

19. **Occasional Transaction** means the transaction performed by the Company in the course of economic or professional activities for the purpose of provision of a service, the sale of goods, or the distribution thereof in another manner to the User outside the course of an established Business Relationship.
20. **Guideline**(s) refers to this document and all of its annexes. The Company's internal control procedure and its Risk Assessment Policy, which outlines a risk-based strategy to managing ML/TF risks and suitable appetites, are among the other items covered by the Guidelines.
21. **Management Board** refers to the management board of the Company.

22. **CEO** means Chief executive officer of the Company.
23. **MLRO** means Money Laundering Reporting Officer, who is appointed to the Company as a person responsible for receiving internal disclosures and making reports to the Financial Crime Investigation
24. **The Employee** means the Company´s employee, including persons which are involved in application of this Policy in the Company.

4. Roles and Responsibilities

1. **The Board** is responsible for maintaining a strong compliance culture with anti-money laundering (AML) and counter-terrorist financing (CTF) regulations. They guarantee that both Board members and employees have all the information about these requirements and understand their responsibilities. The Board also ensures that relevant risk factors are fully considered in the company's decision-making processes.

Specifically, the Management Board has ultimate responsibility for preventing the misuse of the company's services for money laundering or terrorist financing. Their responsibilities include:

- Establishing and maintaining AML processes, procedures, risk management, and control mechanisms.
- Adopting the AML Policy and other internal guidelines and instructions.
- Setting the company's AML guidelines.
- Appointing a Money Laundering Reporting Officer (MLRO) and ensuring the MLRO has the necessary authority, resources, and expertise to fulfill their role.
- Allocating sufficient resources to effectively implement the AML Policy and related documents, and maintaining the organizational structure.
- Ensuring that all relevant employees undergo annual AML training.

The following policies, procedures and reports are to be approved by the Board of Directors and must be reviewed and where necessary updated at least annually:

1. AML/CTF Policy;
2. Risk Management Policy;
3. Governance Policy and Code of Conduct;
4. Compliance Policy;
5. Consumer Rights and Complaints Handling Policy;
6. Information Security Policy;
7. Business Continuity Policy;
8. Annual Compliance Report; and
9. Annual Risk Assessment.
10. Travel Rule Policy

As the senior-most management body, the Board is responsible for approving and handling risk management and compliance policies. They must have a thorough awareness of money laundering concerns, including access to timely, complete, and accurate risk assessment information in order to make informed decisions. The Board, in collaboration with the General Manager, should appoint a competent AML Officer with overall responsibility for the AML function, and ensuring that this senior officer has adequate authority to successfully handle concerns with the Board, the General Manager, and the business units.

The Board is also tasked with overseeing the company's overall AML/CTF compliance policy, ensuring that adequate resources are provided for staff training and the implementation of risk systems. Additionally, the Board will review and consider quarterly compliance reports presented by the AML Officer.

2. **The General Manager** holds a pivotal role, overseeing daily operations to ensure efficiency and compliance with regulatory standards. Possessing sufficient seniority and knowledge of the institution's money laundering and terrorist financing risk exposure, the General Manager is responsible for making decisions that affect the platform's risk profile. They receive and consider monthly compliance reports from the AML Officer and authorize changes based on recommendations when necessary. Additionally, they receive reports on significant changes that could pose risks to the organization. The General Manager assists in preparing the AML program and ensures the platform adheres to AML and Counter-Terrorist Financing (CTF) regulations. Key duties also include developing and implementing strategic plans to foster growth, managing financial health through budgeting and reporting, mitigating operational risks, leading the team to create a positive work environment, and engaging with stakeholders to maintain strong relationships. Ensuring an excellent user experience and continuously improving the platform based on feedback and industry trends are also critical aspects of their role.

3. **The AML Officer** holds a pivotal role, overseeing daily operations to ensure efficiency and compliance with regulatory standards. Possessing sufficient seniority and knowledge of the institution's money laundering and terrorist financing risk exposure, the AML officer is responsible for making decisions that affect the platform's risk profile. Additionally, they assist in preparing the AML program and ensures the platform adheres to AML and Counter-Terrorist Financing (CTF) regulations. Key duties also include developing and implementing strategic plans to foster growth, managing financial health through budgeting and reporting, mitigating operational risks, leading the team to create a positive work environment, and engaging with stakeholders to maintain strong relationships. Ensuring an excellent user experience and continuously improving the platform based on feedback and industry trends are also critical aspects of their role.

Key responsibilities of the MLRO include:

a. Policy Management:

- Producing and updating the company's AML/CTF policies as needed.
- Monitoring and verifying ongoing compliance with these policies and external

regulations.

b. Advisory and Support:

- Providing advice and support to the company's staff and board members on AML/CTF rules.
- Informing and training relevant personnel on AML/CTF regulations.

c. Investigations and Reporting:

- Investigating internal notifications of suspicious activities and determining their legitimacy.
- Filing relevant reports (SARs) with regulatory authorities in accordance with local requirements.

d. Procedure and Guideline Assessment:

- Regularly assessing the effectiveness of the company's procedures and guidelines to prevent money laundering and terrorist financing.
- Identifying incidents and taking appropriate measures as per company policy.

e. Liaison Duties:

- Coordinating with third-party KYC/KYB service providers for initial screenings of business partners.

f. Quarterly Reporting:

Reporting quarterly to the Management Board with details such as:

- Number of customers under various risk classifications.
- Hits related to sanctions lists and applied measures.
- Identification of PEPs (Politically Exposed Persons) and their associates. (Currently we are not onboarding any PEPs)
- Internal notifications on suspicious activities.
- Reports filed with the Italian Unità di Informazione Finanziaria(UIF).
- Requests for information from the UIF.
- Confirmation that risk assessments and policies are up to date.
- Adequacy of staffing and training in respect of AML measures.
- Addressing any identified inadequacies.

4. **Other staff members** are responsible for familiarizing themselves with the AML/CTF Policy and other internal procedures relevant to their roles, ensuring they understand their responsibilities. They must adhere to AML/CTF procedures and report any suspicious activity to the AML Officer. Employees are expected to act with the foresight and competence appropriate to their positions, supporting the company's goals and ensuring the financial system is not used for money laundering or terrorist

financing. The Company assesses the suitability of employees before they begin their roles, providing relevant training.

To meet these expectations, employees are required to:

g. Comply with all requirements outlined in the AML/CTF Policy and related documents.

h. Collect necessary customer information according to their functions and responsibilities.

i. Promptly report any unusual information, situations, activities, transactions, or attempted transactions to the MLRO, regardless of the amount or whether the transaction was completed.

j. Refrain from informing customers if they or others are the subject of a report or if a report has been or may be filed.

k. Complete the appropriate AML training required for their positions.

5. Comprehensive Measures Implemented by Web3 Solutions to Prevent Money Laundering and Terrorist Financing

Web3 Solutions S.r.l has established a robust framework to combat money laundering and terrorist financing in strict adherence to Italian regulations and international standards adhering to adheres to both Italian and EU regulatory requirements, such as those outlined by MiCAR and AMLD5.

5.1 Identification of the customer and beneficial owner:

Web3 Solutions S.r.l has established structured procedures for identifying business applicants, ensuring that their identities are confirmed using the documents, data, and information (as per Appendix 2) obtained from reliable and independently verified sources. Web3 Solutions S.r.l identifies and verifies the customer and beneficial owner on its platform, takes up reasonable measures to verify their identity to ensure a thorough understanding of who the beneficial owner is. In the case of corporate entities, reasonable measures are taken to understand their ownership and control structure. The following are the identification and verifications performed on each onboardings:

i. determines whether the customer is acting on his own name or under control:

ii. if the customer is acting through a representative, identifies customer's representative;

iii. identifies customer (natural person);

iv. identifies customer (legal entity);

v. identifies customer’s (legal entity) beneficial owner;

vi. collects information about customer’s (legal entity) director;

vii. collects information on the ownership and management structure of customer legal entity, nature of its business;

viii. collects information on the purpose and intended nature of the business relationship of a customer (natural or legal person);

ix. Collects information on source of funds, for higher-risk customers, additional details may be

required on how the customer accumulated their wealth over time (e.g., inheritance, business income, employment income, Investments).

x. Collects proof of address of Customer's (legal entity) UBO and director

xi. verifies the identity of the customer and the beneficial owner on the basis of documents, data or information obtained from reliable and independent sources;

xii. conducts additional identity verification steps for high-risk consumers, such as politically exposed persons (PEPs) (Currently we are not onboarding any PEPs)

xiii. identify customers from high-risk jurisdictions, and customers engaged in high-risk activities.

xiv. Collects information on the source of funds as in section 9 of 5.1, wealth, financial history and supporting documentation of high-risk customers to ensure legitimacy.

xv. regular monitoring of customer's business relationship – transaction monitoring;

xvi. conducts adverse media screening to identify any negative information or news related to the customer or beneficial owner, which could indicate a higher risk.

xvii. continuous review and update of documents, data or Assess the customer's and beneficial owner's geographic risk, considering criteria such as the customer's place of residency, the country in which the business is performed, and any other relevant countries.

xviii. information collected during the customer and beneficial owner identification process – ongoing due diligence.

Category	Attribute	Details we collect
General Information	Client Type	Individual / Legal Entity
	Full Legal Name	Customer's full name (or registered name for entities).
	Registration/ID Number	Passport/ID number for individuals or registration number for entities.
	Date of Incorporation / Birth	Date of registration (for entities) or date of birth (for individuals).
	Country of Registration / Nationality	Country of incorporation (for entities) or nationality (for individuals).
	Address	Complete residential or business address.
	Contact Information	Email, phone number, and any secondary contact details.
Business Details	Sector/Industry	Industry or business sector of the customer.
	Expected Business Volume	Anticipated monthly or annual

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

		transaction volume.
	Business Activity Description	Brief description of the customer's business activities.
Ownership and Control	Ownership Structure	Description or diagram of the ownership structure, if applicable.
	UBO Names	Names of all Ultimate Beneficial Owners (with >25% ownership).
	UBO Ownership Percentage	Percentage of ownership held by each UBO.
	Intermediaries	Any intermediary entities with >25% ownership.
	Control Verification Documents	Documents proving UBO ownership (e.g., shareholder register).
	Director Name	Name of the Entity's Director
Compliance Checks	Sanctions List Screening	Results of sanctions screening for both the customer, UBOs and Director.
	PEP Check	Results of PEP screening for both the customer, UBOs and Director
	High-Risk Jurisdiction Check	Flag if the customer is linked to high-risk jurisdictions.
	Negative Media Screening	Results of adverse media checks.
Documents	Identity Documents	Passport or Residential ID (for individuals) or Certificate of Incorporation (for entities).
	Proof of Address	Utility bills, lease agreements, bank statement, municipalities tax bill or equivalent.
	Business Registration Documents	Articles of Association, Tax Identification Number (TIN) document, or equivalent.
	Transaction Source Verification Documents	Bank statements, trading volume statement or other proof of source of funds.
Risk Assessment	Risk Score	Assigned based on risk-based approach (Low/Medium/High).
	Risk Justification	Brief explanation of why the customer is assigned a particular risk level.

		(Customer providing services or making transactions with high risk Jurisdictions)
	Risk Mitigation factors	List all risk factors
Decision	Compliance Officer Approval	Name and signature of the officer approving or rejecting the onboarding.
	Final Decision	Accept / Reject
	Comments	Notes or clarifications supporting the decision.

5.2 when there is no possibility to fulfill the customer and beneficial owner identification requirements – suspension of transactions, refusal to establish or termination of business relationship;

5.2.1 Signs indicating the inability to fulfill the customer and beneficial owner identification requirements.

i. Inconsistent or insufficient identifying information, even when asked for clarification.
ii. Inability to authenticate provided documentation.
iii. Altered, forged, or suspicious documentation
iv. Customer or beneficial owner reluctance or refusal to provide necessary information.
v. Refusal to disclose the beneficial owner's identity.
vi. Complex ownership structure conceals the beneficial owner.
vii. Transactions inconsistent with the customer's profile.
viii. Large or unusual transactions without clear purpose.
ix. Association with sanctioned jurisdictions.
x. Adverse media reports indicating criminal activities.
xi. Negative reports about the customer or beneficial owner in reputable sources.
xii. Business models or operations are not well understood or appear suspect.

The following table provides a detailed overview of positive and negative indicators that determine the ability or inability to meet customer and beneficial owner identification requirements:

Positive Signs	**Type**	**Indications**
(Customers exhibiting all or most positive signs can be onboarded)	Clear Documentation	Valid government-issued ID and proof of address provided.
	Full Ownership Data	UBO information is complete, including ownership percentage and supporting documents.
	Verified Data	No discrepancies in KYC data;

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

		documents match the declared details.
	AML Screening Clear	Sanctions, PEP, and adverse media screenings return no red flags.
	Cooperation	Customer responds promptly to requests for additional information or clarification.
	Clear Source of Funds	Documents proving legitimate sources of funds (e.g., bank statements) are provided.

Negative Signs (If negative signs outweigh positive ones, the onboarding should be rejected to mitigate regulatory and reputational risks.)	**Type**	**Indications**
	Missing Documents	Failure to provide valid proof of ID or address.
	Incomplete UBO Data	UBO ownership percentages or control details are missing or unclear.
	Discrepancies	Mismatched or inconsistent information across documents or between declared data and evidence.
	Sanctions Red Flag	Customer or UBO appears on sanctions lists (e.g., OFAC, EU).
	Adverse Media Hits	Negative media mentions related to fraud, corruption, or criminal activities.
	No Cooperation	Customer delays or avoids responding to KYC/AML requests.
	Untraceable Funds	Source of funds or wealth cannot be verified with supporting documents.

PEP or High-Risk (Decision based on EDD results and documentation findings)	Customer or UBO is a politically exposed person (PEP) or linked to high-risk jurisdictions.

5.3 applying customer and beneficial owner identification tools to existing customers;

5.4 suspension of a suspicious monetary operation or transaction;

5.5 reporting suspicious monetary operations or transactions to UIF;

5.6 a notice on virtual currency exchange operations or transactions in virtual currency where the value of such monetary operation or transaction is equal to or greater than EUR 1,000 or currency and virtual currency equivalent, whether the transaction is carried out in one or several interrelated transactions;

5.7 investigation of complex structure, unusually large and suspicious transactions;

5.8 Red flags associated with suspicious transactions;

5.8.1 Red Flag indicators related to transactions

i. Configure VA transactions for small amounts or amounts below record-keeping or reporting thresholds.

ii. Making multiple high-value transactions

iii. Depositing VAs to an exchange and then often immediately

iv. Accepting funds suspected of being stolen or fraudulent

5.8.2 Red Flag indicators related to transaction patterns

i. To start a new relationship with a VASP, make a large initial deposit and fund the entire stake on the first day of opening. The client starts to process the total amount or a large part of the amount on the same day or the next day, or if the client withdraws the entire amount the next day.

ii. A new user tries to swap the VA as a whole balance or withdraw the VAs and tries to send the entire harmony out of the platform.

iii. Operations involving the use of more than one VA without a correct and logical job description.

iv. Making frequent transfers to the same VA account by more than one person, by one or more people from the same IP address, or by large amounts of money in a specified period

v. Relatively small amounts of transactions from many unrelated wallets then transfer to another wallet or full exchange for fiat currency.

vi. Realizing the VA-fiat currency exchange with a potential loss

vii. They convert large amounts of fiat currency to VAs or a large quantity of VA type to other VA types without a logical job description.

5.8.3 Red flag indicators related to anonymity

i. Transactions performed by a client with multiple VA types despite higher anonymity VAs, such as anonymized cryptocurrency (AEC) or privacy coins.

ii. Moving a VA is running on a public, transparent blockchain like Bitcoin to a central exchange and then immediately swapping it for an AEC or privacy coin.

iii. Customers working as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites

iv. Abnormal transaction activity of VAs converted to cash on exchanges from wallets associated with the P2P platform without any logical job disclosure.

v. VAs transferred to or from wallets showing previous activity patterns related to the use of VASPs running shuffling or rolling services or P2P platforms.

vi. Transactions using scrambling and disruption services suggest the intention to prevent illegal fund flows between known wallet addresses and darknet markets.

vii. Money is withdrawn from a VA address with links to direct and indirect exposure to known questionable sources, including Darknet markets, scrambling services, suspected gambling sites, illegal activities, and reports of theft.

viii. Use of decentralized hardware or paper wallets to move VAs across borders.

ix. Users who register Internet domain names on the VASP platform through proxies or use domain name registrars (DNS) that hide or remove domain name owners.

x. Many seemingly unrelated VA wallets are controlled from the same IP address (or MAC address) and may include the use of shell wallets registered to different users to hide their relationship with each other.

xi. The use of VAs whose design is poorly documented or associated with other means of implementing fraudulent schemes, such as possible fraud or pyramid schemes.

xii. Receiving or sending money to VASPs whose CDD or know your customer (KYC) processes are weak or absent.

5.8.4 Red Flag indicators about senders or recipients

i. To create separate accounts under different names to circumvent the restrictions on trading or withdrawal limits imposed by VASPs.

ii. Transactions initiated from untrusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously marked as suspicious

iii. Frequent attempts to open an account within the same VASP from the same IP address.

iv. Regarding merchants / corporate users, Internet domain registrations are different from the organization's jurisdiction or jurisdiction, with an inefficient process for domain registration.

v. During the CDD process, irregularities were observed, missing or insufficient KYC information or a client denying requests for KYC documents, or questions regarding funding sources.

vi. Do not know or provide false information about the sender/recipient, transaction, source of funds, or relationship with the counterparty.

vii. The client provided forged documents or edited photos and/or ID documents as part of the recruitment process.

viii. Discrepancies arise between the IP addresses associated with the customer's profile and the IP addresses where transactions were initiated.

ix. A client older than the average age of platform users, a client opens an account and executes many transactions, suggesting their potential role as a VA coin mule or a victim of aged financial exploitation.

x. Customer frequently changes their credentials, including email addresses, IP addresses, or financial information, indicating an account takeover against a client.

5.8.5 Red flag indicators for fund or wealth source

i. Dealing with VA addresses or bank cards linked to known fraudulent, extortion or ransomware schemes, sanctioned addresses, darknet markets, or other illegal websites.

ii. VA transactions arising from or for online gambling services.

iii. Using one or more cards linked to a VA wallet to withdraw large amounts of fiat money.

iv. Lack of transparency or insufficient information about the source and owners of funds, such as funds placed in the Coin Offerings (ICO) or online payment system with credit / prepaid cards followed by instant withdrawal.

v. A customer's funds are obtained directly from third-party mixing services or wallet vaults.

vi. Most of a client's wealth resource is to VAs, ICOs or fraudulent ICOs, etc. It is obtained from the investments made.

vii. A client's wealth source is disproportionately derived from VAs from other VASPs that do not have AML / CFT controls.

5.8.6 Red flag indicators related to geographical risks

i. The client's funds originate from or are sent to an exchange that is not registered in the client's jurisdiction.

ii. If the customer uses a VA stock exchange or MVTS based abroad in a high-risk jurisdiction known to have no or insufficient AML / CFT regulations for VA units, including inadequate CDD or KYC measures.

iii. The customer sends money to VASPs operating in jurisdictions that do not have VA regulations or implement AML / CFT controls.

iv. The client sets up or moves offices in jurisdictions that do not have or legal regulations governing VAs.

5.9 information storage for a specified period of time;

5.10 designating staff responsible for implementing measures to prevent money laundering and / or terrorist financing;

5.11 staff training;

i. All employees and individuals managing customers' business will receive sufficient training regarding Prevention of Italian Money Laundering Act and the relevant laws and regulations.

ii. The level of training that is given will be based on suitability for the employee's position and level

of seniority within the organization.

5.12 implementation of internal systems to enable prompt response to inquiries from the Unità di Informazione Finanziaria(UIF) via secure channels and ensuring full confidentiality of inquiries;

5.12 confidentiality of the information provided to the UIF;

5.13 setting internal policies, procedures and controls in place;

5.14 submission of information on the beneficial owners of the Depository Virtual Currency Wallet Operator and Virtual Currency Exchange Operator to the Legal Entities Participant Information System (JADIS) Manage;

6. Company's Structure

6.1 Parent Company: Lunu Solutions GmbH

Type: Limited Liability Company (GmbH)

Location: Based in Germany (or the jurisdiction where it is incorporated).

Role: As the parent company, Lunu Solutions GmbH holds complete ownership of Web3 Solutions S.r.l, providing strategic direction, financial support, and operational oversight.

6.2 Subsidiary: Web3 Solutions S.r.l

Type: Limited Liability Company (S.r.l)

Location: Based in Italy.

Ownership: 100% owned by Lunu Solutions GmbH, making it a wholly owned subsidiary.

Role: Web3 Solutions S.r.l operates as an independent entity that focuses on specific business activities related to virtual assets and blockchain technology. As a subsidiary, it benefits from the resources, expertise, and backing of Lunu Solutions GmbH.

6.3 Names of the managers and members of the Board of Directors

i. Roman Rashimas - Director

ii. Pavlo Denysiuk - Member of the Board of Directors

7. BUSINESS WIDE ML / TF RISK ASSESSMENT

7.1 In the business wide ML / TF risk assessment (hereinafter – ML/TF risk assessment), the Company will analyze potential threats and vulnerabilities to money laundering and terrorist financing to which the business is exposed.

7.2 When identifying whether there is higher risk of money laundering and/or terrorist financing the Company will assess at least the following:

7.2.1 customer risk factors:

i. the business relationship of the customer is conducted in unusual circumstances without any apparent economic or lawful purpose;

ii. the customer is resident in a high risk third country (as per Appendix 1);

iii. legal persons or entities without legal person status acting as asset-holding vehicles;

iv. legal entity has nominee shareholders or issued bearer shares;

v. the ownership structure of legal person appears unusual or excessively complex given the nature of the legal person's business;

The risk assessment requires that the Company knows its customers and the nature of their business. This is not limited to identification process or record keeping, but it is about understanding customers, including their activities, transaction patterns, and how they operate.

7.2.2 product, service, transaction or delivery channel risk factors:

i. a product or transaction might favor anonymity;

ii. business relationship or transactions are established or conducted without the physical presence;

iii. payments are received from unknown or unassociated third parties;

iv. products and business practices, including delivery mechanism, are new and new or developing technologies are used for both new and pre-existing products;

v. transactions in oil, weapons, precious metals, tobacco products, cultural artefacts and other objects of archaeological, historical, cultural and religious significance or of rare scientific value, as well as in ivory and protected species.

The Company will identify products and services or combinations of them that may pose an elevated risk of money laundering or terrorist financing. Products and services that can support the movement and conversion of assets into, through and out of the financial system may pose a high risk.

7.2.3 geographical risk factors:

i. countries identified, on the basis of data of reports or similar documents by the Financial Action Task Force (FATF) or a similar regional organization, as having significant non-compliances with international requirements in their anti-money laundering and/or counter financing of terrorism systems;

ii. countries identified, on the basis of data by governmental and universally-recognized non-governmental organizations monitoring and assessing the level of corruption, as having significant levels of corruption or other criminal activity;

iii. countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;

iv. countries provide funding or support for terrorist activities, or have designated terrorist organizations operating within their country.

v. Certain geographic locations potentially pose an elevated risk for money laundering and

terrorist financing.

7.3 The ML / TF risk assessment results may identify increased-risk situations for which additional risk mitigation controls and monitoring may be required.

7.4 The ML / TF Risk assessment is a written document based on statistical data which outlines risk mitigation controls in place and their effectiveness so that residual risk can be assessed for each risk identified.

7.5 The results of the ML / TF risk assessment and remediation plan are communicated to Management Board who will need to approve remediation plan and assign responsible people to carry it out.

7.6 ML / TF risk assessment is carried out every year.

8. Internal Control Procedures

8.1 The Company must set out AML/CFT internal controls covering:

1. Roles and responsibilities over ML/TF prevention, including access to all information needed to perform daily duties according to roles and applicable laws;
2. Risk assessment, risk controls
3. Identification and verification of customer and beneficial owner;
4. Sanctions and Politically Exposed People (PEP) screening;
5. Ongoing due diligence;
6. Transaction monitoring;
7. Suspicious activity reports (SAR) to the Unità di Informazione Finanziaria(UIF);
8. Record keeping requirements;
9. Management of information logs;
10. Management Board information system to communicate internal and external information which might have impact to make decisions regarding ML/TF risk management.
11. Constant employee training.
12. Proper safeguarding of confidential information obtained while implementing AML/CTF program.

8.2 Internal controls in place and related procedures must be updated when:

- European Commission completes supranational ML/TF risk assessment (announced here http://ec.europa.eu);
- Italy completes national ML/TF risk assessment;
- The UIF orders to tighten internal control procedures;
- There are significant changes in management structure and business nature;
- Gaps are identified during periodical quality assurance process.

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

9. Customer Risk Scoring

9.1. Customers are classified with a risk level: low, medium, high risk and prohibited.

9.2. Customer risk scoring procedure and risk scoring matrix are provided in the On-boarding procedure.

9.3. When a customer is identified as high-risk, they are subject to appropriate enhanced due diligence measures.

9.4. For new customers risk scoring is performed before entering business relationship. The Company performs risk scoring for existing customers during ongoing due diligence.

Risk Level	Description	ODD Period	Monitoring Requirements
Low Risk	Transparent sources of funds, verifiable information, low-risk jurisdictions.	12 months	Simplified due diligence (SDD); regular monitoring for compliance with the declared transaction profile.
Medium Risk	Slightly complex ownership structures, moderate AML/CFT compliance jurisdictions, occasional anomalies.	9 months	Standard due diligence (CDD); increased frequency of transaction reviews and monitoring for unusual activity.
High Risk	High-risk industries, weak AML/CFT jurisdictions, unusual or inconsistent transaction patterns.	6 months	Enhanced due diligence (EDD); frequent and detailed monitoring, including source of funds and ownership checks.
Prohibited	Linked to illegal activities, sanctioned entities, or non-compliance with minimum requirements.	Not Applicable	Customer is ineligible for onboarding or service continuation; immediate reporting to authorities if required.

9.5 Customer Due Diligence

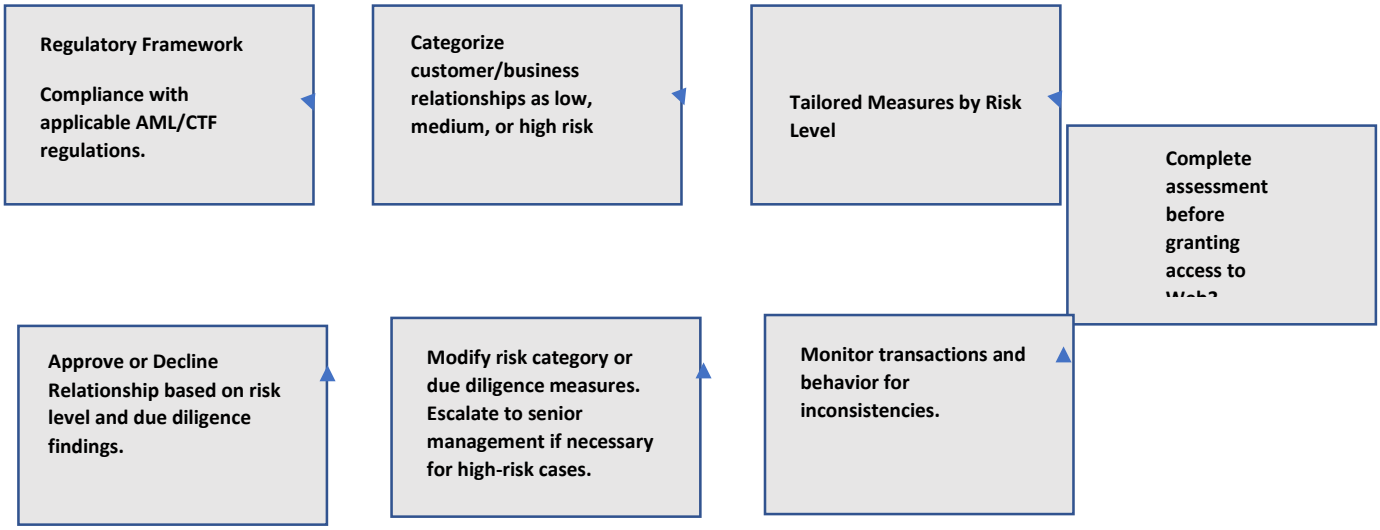
9.5.1. Risk-Based Approach

In accordance with various provisions of the applicable regulations, Web3's retailer and customer due diligence measures and AML/CTF controls involve the use of evidence-based decision-making to address the risks of money laundering and terrorism financing.

Web3 will categorize each business relationship into low, medium, or high-risk categories and will tailor due diligence measures, KYC requirements, and approval protocols based on these categories. The risk category of each customer relationship must be based on the assessment of the AML/CTF risks posed by the customer, including information about the nature of the business relationship, associated countries, geographical areas, products or services offered to such customers, transactional volumes, consistency of behavioral patterns, and other pertinent factors.

The assessment of the risk level to be assigned to a retailer or customer will take place before the retailer or customer is able to use Web3 services and subsequently when new information about the customer becomes available. During the course of each business relationship, Web3 will continue monitoring the development of the risks and adapt its assessment according to any significant changes affecting retailer and customer risk categorization.

Web3's adoption of a risk-based approach will determine the extent of the client due diligence measures, the frequency of the due diligence activities, and, where applicable, the required level of approval needed to accept or decline the customer relationship.



9.5.2. Customer Categorization and Acceptance

Web3 is a Business-to-Business (B2B) platform and will have the following category of customers:

- Retailers, legal persons who register via the Console and complete KYB requirements to use Web3 Services.

In order to use Web3 Services, all Retailers must fulfill appropriate registration and verification steps, including providing required onboarding information, accepting the relevant terms and conditions, privacy policy, and other policies, and passing the sanctions screening.

In summary, Web3's onboarding flow for retailers includes the following steps and checks for each new

retailer:

- Provide the following documents:
  1. Copy of an ID or passport of every director and shareholder/UBO (who owns more than 25% of shares) and their proof of addresses;
  2. Proof of the company address. We accept the following address verification documents, issued within 90 days;
     a. Paper and digital bank statements;
     b. utility bills - electricity, water, waste management, fixed internet or phone bills (no mobile phone bills and insurance letters), etc.
     c. government issued letters - such as letters from government agencies, tax bills, etc.
  3. Certificate of the Registration of Incorporation/ registry extract;
  4. Memorandum of articles of Association / Constitution / By-Laws;
  5. Confirmation of an active status of the company (if it's not indicated in Registration Extract);
  6. Confirmation of the director (if it is not indicated in Registration Extract);
  7. Ownership structure i.e., list of all Shareholders with the specified number of shares;
- Accept terms and conditions and privacy policy
- Using KYC tools with sanctions scanning and document verification features (SumSub as a primary tool), we validate:
  1. Whether the person is on the sanctions/PEP/other high risk (e.g. HMT, OFAC, UN, and EU)) list;
  2. Whether the document is authentic and not expired;
  3. Whether the document is reported as stolen or lost;
  4. Whether the registration information that we have on file is the same as the information on the document uploaded by the retailer.
- Web3's onboarding flow for customers includes the following steps and checks for each new customer:
  1. Provide a Copy of an ID or passport.
  2. Provide a selfie.
  3. Whether the document is authentic and not expired.
  4. Whether the document is reported as stolen or lost.
  5. Whether the registration information (date of birth, nationality, passport number, full name, document type) on file matches the information on the document uploaded by the customer.
- Accept terms and conditions, terms of use, and privacy policy.

If inconsistencies or potential risks are detected during the onboarding process, they must be researched and resolved before the retailer or the customer is able to use the Web3 services. As a method of

additional research or verification, Web3 may contact the retailer and clarify the inconsistent circumstances, ask for alternative documents to be provided, research whether there are any adverse media or online information about the persons (especially for potential PEP clients), conduct a video interview, and employ other methods, depending on the nature of the circumstances that triggered the "red flag." As a result of this additional research, the following outcomes are possible:

- The inconsistencies could be resolved and the retailer will be confirmed as a medium risk retailer;
- The risk flags are confirmed and then the retailer is categorized as a high-risk retailer and should be subject to the EDD;
- The retailer relationship is declined, for example, if the customer never provided additional information or if it has been confirmed that the customer poses too high risk for Web3 and cannot be accepted. The Italian MLRO will make an appropriate decision, whether the SAR should be filled.

As a summary of the above, Web3 will do the following checks at the moment of retailer onboarding for all retailers (e.g. retailer registration):

Data provided by the Retailer	**"Silent checks"**	**Follow up, if there is an alert**
Copy of an ID or passport of every director and shareholder/UBO (who owns more than 25% of shares) and their proof of addresses	• name is scanned against all WorldCheck lists for all countries for SDN and PEPs • name is scanned against negative media references (corruption scandals, bankruptcies, litigations, change in control, M&A announcements) • name is scanned for obviously false names, e.g. Coca-Cola, Peter Pan, celebrity names, obviously abusive and oblivious names • Validation that the Retailer's Representative is at least 18 years old • Block Representatives resident in Prohibited Jurisdictions • Flag cases where nationality is different	• If there is a partial match, account is flagged and reviewed, additional info from Merchant requested • Block if the Retailer's Representative in under 18

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

	from residence country (excluding mismatches between EU countries)	
Proof of the company address	• Ensure that the address is from an eligible country	• Flag high risk countries, block disputed territories and territories where we don't offer services (eg. Syria, Crimea, Kosovo)
Certificate of the Registration of Incorporation/ registry extract	• Flag inconsistencies	
Memorandum of articles of Association / Constitution / By-Laws	• Flag inconsistencies	
Confirmation of an active status of the company	• Flag inconsistencies	
Confirmation of the director	• Flag inconsistencies	
Ownership structure	• Flag inconsistencies	
E-mail	• Confirm email by reverse link • Detect temporary emails and bots • Scan emails with social media scanning tool for references in commercial registers, social media and other public databases	• Flag bots and temporary emails

As a summary of the above, Web3 will do the following checks at the moment of customer onboarding for all customers (e.g. customer registration):

Data provided by the Retailer	**"Silent checks"**	**Follow up, if there is an alert**
Copy of an ID or passport	• Name is scanned against all WorldCheck lists for all countries for SDN and PEPs • For suspected PEPs and SDNs, the name is	• If there is a particular match, account is flagged and reviewed; •

	scanned against negative media references (corruption scandals, bankruptcies, litigations, change in control, M&A announcements) • Name is scanned for obviously false names, e.g. Coca-Cola, Peter Pan, celebrity names, obviously abusive and oblivious names • Validation that the client is 18 years old • Block North Korea and other prohibited jurisdictions • Flag cases where nationality is different from residence country	• Block if the client if under 18 • In cases where nationality is different from residence, ensure we will ask for proof of visa/legal status
Selfie	• Face is matched against passport	• Flag inconsistencies

As an example, where the customer is residing in Italy or another EU member state with a robust AML/CTF regulatory framework and using a virtual currency address known to be part of a regulated virtual asset exchange or a well-established custodian, such a scenario can be described as behavior consistent with multiple low-risk indications under MiCA and Italian AML/CTF regulations. Conversely, examples of higher risk scenarios include instances where a customer makes a payment from a wallet flagged as High Risk by blockchain tracking tools or submits an unreasonable request to customer support to process a highly unusual transaction. In such cases, Web3 is equipped to detect suspicious activities in close to real-time and to request additional information from the customer before enabling the transaction in question.

In cases where there is an indication that the customer represents a higher AML/CTF risk (e.g., due to material discrepancies identified during customer account review or flagged transactional behavior), such customers must be requested to provide additional information about themselves. If the High-Risk categorization is confirmed, the MLRO will provide formal approval to confirm or decline the business relationship.

With respect to understanding the nature of the business relationship, Web3 will ensure that the planned business activities of retailers and customers who onboard online are clearly defined and compliant with MiCA and Italian AML/CTF regulatory requirements. Web3's Terms and Conditions and Terms of Use,

which must be accepted by all retailers and customers, will specify acceptable and prohibited activities, as well as detailed guidelines regarding the use of Web3's services. This approach ensures compliance and risk mitigation, as Web3 will provide a standardized and limited set of services specifically tailored to meet the regulatory requirements under MiCA and Italian law.

10. Identification of The Customer and The Beneficial Owner

10.1. The Company will take measures to identify the customer and the beneficial owner as well as verify their identity:

10.1.1 before:

- executing occasional virtual currency exchange transactions or operations in virtual currency with funds equal to or above EUR 1,000 (KYT) or currency/virtual currency equivalent.
- occasional depositing or withdrawing of virtual currency amounting to or above EUR 1,000 (KYT) or currency/virtual currency equivalent. (one or bundle of transactions/ linked transactions)
- transaction is carried out in one or more interrelated transactions (the value of the virtual currency being determined at the time of the monetary transaction or operation) unless the customer and beneficial owner have already been identified.

10.1.2. when there are doubts about the veracity or authenticity of the previously obtained identification data of the customer and the beneficial owner;

10.1.3. in any other case when there are suspicions that an act of money laundering and/or terrorist financing is, was or will be carried out;

10.1.4. In any case if customer is a high risk.

10.2. The Company will carry out customer's and beneficial owner's identification by applying a risk-based approach using:

1. customer identification tools and customer due diligence (CDD) procedures;
2. additional customer authentication tools and procedures for enhanced due diligence (EDD);
3. simplified customer identification tools and procedures for simplified due diligence (SDD).

10.3. In case the Company is unable to meet the requirements set out in point 11.1.1, company will carry out the money laundering and/or terrorist financing threat assessment. After detecting the risk of money laundering and/or terrorist financing (ML/TF), the Company will report the suspicious monetary operation or transaction to the UIF.

11. Risk factors

The risk classification of the retailers and customers is based on the following criteria:

a) Country of origin/operation. Country Risk Matrix is provided.

b) Legal form of the retailer. Certain legal forms pose an inherently higher risk of money laundering/terrorism financing. For example, entities with complex legal structures, such as trusts, foundations, non-profit organisations and charities may pose additional money laundering/terrorism financing risks. For retailers categorised as High Risk due to their complex legal structure, the legal form of the entity, the nature of the business activity, the identity of the UBOs and proxy-holders will be analysed with increased scrutiny as part of enhanced due diligence. State-owned and state-invested entities will be categorised as PEPs. Retailers with share capital in bearer form are prohibited.

c) Business line of the retailer. Individual retailers with low-value consistent transactional patterns normally represent a lower risk. Whenever a retailer is engaged in one of the following activities, its risk category has to be assessed on an individual basis, since the inherent risk of the below-mentioned activities is considered to be above average for Web3 business model:

- E-cigarettes
- Products relating to dating services
- Regulated Cannabis Industry
- Agriculture / Farming
- Adult content and services
- Alcohol
- Art Dealers
- Boat Dealers
- Business active in government procurement, i.e., those whose business is selling to government or state agencies
- Cash-intensive business, including beauty parlours, newsagents, restaurants, bars, nightclubs, public houses, takeaways, and car washes
- Chemical Manufacturing
- Clothing Manufacturing
- Construction and (large) infrastructure
- Crowdfunding
- Cyberlocker (an internet service that allows users to store and share files online)
- Development and other types of assistance
- Entertainment for minors
- Estate Agency Business (EAB)
- Free port operator
- Gaming / Casinos / Amusements
- High value dealers, including luxury goods, precious metals, and precious stones
- Hotels and accommodation in high risk countries (as per Appendix 1)
- Language Schools
- Letting Agency Business (LAB)
- Loan Companies

- Marinas
- Mining and extraction
- Negative option billing
- Non EEA Charities or EEA Non Registered or Non Regulated Charities
- NGO (non-governmental organisations)
- Oil and Gas Pipeline and Related Structures Construction
- Paper Manufacturing
- Petroleum
- Pharmaceutical
- Plastics, Rubber, Metal Manufacturing
- Precious Metal Production
- Privatisation
- Professional football
- Property
- Provision of public goods, utilities
- Securities
- Sugar
- Tobacco
- Travel / Travel Agencies / Tour Operators
- Trust and Company Service Provider (TCSP)
- Vehicle, Motorbikes, Plane, Jet, Boats- trade, maintenance, and repair
- Waste management
- Wealth management & private banking
- Wholesale banking

Some of these will require regulatory authorisation/approvals to conduct activities in the Italy. It will be a part of the process for the CDD to ensure that it understands when a potential customer is conducting regulated activity, and obtains confirmation that it has the requisite licences.

11.1 Prohibited Customers

Business relationships with the following persons are prohibited by Web3:

1. Applicants from prohibited countries or countries included in sanctions lists, as per Appendix 1;
2. Sanctioned individuals;
3. Non-approved PEPs;
4. Retailers or Customers engages in the following businesses:
   -Autographed collectible (memorabilia) businesses
   -Diamond or Precious Metal Investment
   -Defence / Military Related
   -Hypnosis services
   -Mini-bonds

-Multi-Level Marketing (MLM)
-Nutraceuticals businesses
-Psychic service
-Shell Banks
-Telemarketing Bureaus and Other Contact Centers
-Unregulated financial or investment service
-VoIP or telemarketing
-Wine investment

5. Retailers known or reasonably suspected to be involved in criminal or illegal activities or activities that are incompatible with Web3 company values; and
6. Retailers refusing to provide all required KYC information, including information about UBOs or proxy-holders, with specified timeframes. This also applies to customers who provide incomplete or obviously false information, in which case Web3 will be unable to establish and verify the identity of the customer and/or the nature of the business relationship within specified timeframes.

Web3 reserves the right to terminate retailer accounts at its own discretion, for example, when one of the aforementioned prohibitions or indicators of risk is present and unresolved or where it has been established that maintaining the business relationship with such retailer would cause serious operational and/or reputational risk to the company.

11.2 Customer Screening

Web3 Solutions uses SumSub as its primary sanctions and PEP screening system. SumSub sources its data from Thomson Reuters World-Check and LexisNexis. All relevant information available to Web3 Solutions, whether directly obtained from customers or collected independently, is transmitted to these providers via APIs and is used to determine if the customer is included in any sanctions lists. Particular attention is given to the following sanctions lists:

1. UN (Consolidated United Nations Security Council Sanctions List)
2. USA (OFAC SDN List)
3. EU and UK consolidated sanctions lists

Additionally, other sanctions regimes and private lists are considered during the review of screening results and the assessment of customer eligibility (e.g., no-fly lists, adverse media reports, etc.). To analyze screening results, the following indicators are incorporated into the screening logic used by the scanning providers:

- Matching logic: Full name + date of birth + country of birth or nationality at a 90% match. In cases of uncertainty, the biography section of World-Check/LexisNexis can be referenced, particularly for PEP matches. Cases with a 75% to 90% partial match are escalated for manual review by the scanning vendor.
- Cases below 75%: These are generally auto-dismissed, as they are highly likely to be false positives. This aligns with industry recommendations for a “strong match,” as advised by Thomson Reuters and

LexisNexis. For very short names or missing data, the matching algorithms embedded by the providers are automatically adjusted.

- Dismissal indicators: In instances where the World-Check database is incomplete, a Web3 Solutions employee responsible for investigations can manually dismiss matches based on:

1. Significant differences in the name
2. Significant age discrepancies
3. Common names combined with differing dates or places of birth
4. Mismatches in country or occupation

World-Check and LexisNexis data are also manually utilized for screening partners, directors, ultimate beneficial owners (UBOs), proxy holders, and connected parties of partners at onboarding and on an ongoing basis.

Screening Frequency:

1. At onboarding
2. When the customer or partner updates personal information that may affect the screening outcome
3. Monthly

12. Reporting Suspicious Activities and Cooperating with Authorities

At the Senior Management (executive) level, the Italian MLRO (Money Laundering Reporting Officer) is the primary individual responsible for the proper implementation of the AML/CTF program as required under MiCA regulations. The Italian MLRO serves as the main point of contact for regulatory inquiries and cooperation with competent authorities.

The Italian MLRO is the primary contact for competent authorities concerning the reporting of suspicious activities.

Regarding the outcomes of transactional monitoring and ongoing screening, in all cases of partial or inconclusive sanctions list hits or partial or full PEP matches, account activity will be restricted. The retailer or customer will be contacted and requested to provide the necessary information to allow Web3 Solutions to make a fact-based determination on whether such a business relationship is appropriate to continue.

If customers fail to respond, the account activity will remain restricted, and Web3 Solutions will assess whether a suspicious activity report (SAR) should be filed with the competent authorities, in compliance with Italian and MiCA regulations.

The MLRO or their designee will file Suspicious Activity Reports (SARs) with the competent Italian authority the Financial Intelligence Unit (FIU) when they know, suspect, or have reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted. This includes consideration of the relevant customer, their activities, the origin of the funds, the purpose, nature, and procedure of the transaction, in compliance with MiCA regulations.

The MLRO will ensure that Web3 Solutions will:

- Appropriately document its SAR decisions;
- File the Suspicious Activity Report (online or via the prescribed format) as soon as practicable upon detection of suspicious activity;
- Seek the consent of the Financial Intelligence Unit (FIU) to process transactions that have not yet occurred but for which a suspicion has already been formed, in accordance with Italian and MiCA regulations;
- File or amend SARs within the timeframes prescribed by the FIU;
- Create and retain appropriate records of reported activity; and
- Comply with all FIU and other regulatory SAR filing guidance.

Web3 Solutions prohibits all employees, staff, officers, and directors from "tipping off" customers that they are under investigation or that Web3 Solutions has filed a Suspicious Activity Report (SAR) on them.

The Italian MLRO ensures that all employees, staff, officers, and directors receive appropriate training, including the prohibition against "tipping off," as part of the AML/CTF training program.

To minimize the risk of undue disclosure, Web3 Solutions will restrict internal access to SAR filings, related documentation, and other SAR-related information to relevant AML/CTF compliance employees, senior management, and the Board of Directors.

13. AML/CTF Training

Web3 Solutions has established background screening procedures to ensure the integrity of new employees, staff, officers, directors, newly appointed Board members, and senior executives. Web3 Solutions must establish, maintain, and operate appropriate procedures to be assured of the integrity of all new and existing employees, staff, officers, and directors involved in AML/CTF matters.

Web3 Solutions will make reasonable efforts to ensure that its employees, staff, officers, and directors are adequately trained in the applicable aspects of AML/CTF laws and regulations. The training program will cover external regulatory requirements as well as internal Web3 Solutions policies.

New employees, staff, officers, and directors will receive training upon onboarding with Web3 Solutions and annually thereafter. Additionally, role-specific training tailored to particular job requirements will be provided as necessary. All Web3 Solutions S.r.l. employees, staff, officers, and directors supporting regulated activities or interacting with customers will complete a training module, which will include an assessment of their knowledge.

All Web3 Solutions S.r.l. employees, staff, officers, and directors will be trained on the following areas to ensure compliance with AML/CTF applicable laws and MiCA regulations:

- AML/CTF applicable laws, including Customer Due Diligence (CDD) measures, and acquiring adequate information and knowledge to conduct proper CDD checks, screenings, and ensure timely completion;

- PEP (Politically Exposed Persons) policies and procedures;
- Sanctions requirements, including understanding legal restrictions on transactions with sanctioned entities and individuals, and ensuring compliance with international sanctions regimes;
- Prevailing techniques, methods, trends, new products, practices, and technologies used for money laundering and terrorism financing;
- Web3 Solutions S.r.l.'s internal policies, procedures, and controls on AML/CTF, including the roles and responsibilities of employees, staff, officers, and directors in combating money laundering and terrorism financing;
- How to analyse customer information, identify red flags, and detect signs of money laundering during the performance of duties;
- Web3 Solutions S.r.l.'s record retention policy;
- The disciplinary consequences, including civil and criminal penalties, for non-compliance with AML/CTF regulations; and
- "No-tipping-off" requirements, ensuring employees understand the prohibition against disclosing to customers or third parties that they are under investigation or that a Suspicious Activity Report has been filed.

The Italian MLRO, senior management, and Board members of Web3 Solutions S.r.l. will stay informed of relevant changes in AML/CTF applicable laws and regulations, including those under MiCA, to ensure ongoing compliance and alignment with legal requirements.

14. Abandoned and Dormant Accounts

Abandoned and dormant accounts that become active again shall be closely monitored by Web3 Solutions S.r.l. for any indications of suspicious activity, in accordance with AML/CTF requirements under MiCA regulations.

15. Record Keeping

Web3 Solutions S.r.l incorporates comprehensive record-keeping practices designed to ensure full compliance with AML regulations and MiCA requirements by adhering to stringent retention periods, maintaining detailed customer and transaction records, and implementing secure storage and destruction procedures, our policy supports compliance with regulatory standards while safeguarding sensitive information. Additionally, it ensures that all records are readily accessible for audits and inspections, reflecting our commitment to regulatory integrity and operational excellence. We incorporate the details in below table for record-keeping that aligns with Italian and MiCA regulatory standards.

Records	Details
Retention Period	▪ Minimum Duration: Retain records for 8 years after the business relationship ends or transaction completion.
Types of Records	a) Customer Identification and Due Diligence Records:

	▪ Personal details: Name, DOB, nationality, tax ID. ▪ Identification documents: Government-issued ID. ▪ Proof of address: Utility bills, bank statements. ▪ Beneficial ownership details and supporting documents. ▪ Risk classification and rationale. b) Transaction Records: ▪ Transaction details: Date, time, amount, type of VA, counterparties. ▪ Source of funds/assets evidence. ▪ Transaction purpose documentation. c) Suspicious Activity Monitoring: ▪ Records of flagged transactions. ▪ Enhanced due diligence (EDD) documentation. ▪ Submitted STRs. d) Training Records: ▪ Attendance logs of AML/CFT training. ▪ Training content and provider details. e) Audit and Monitoring Records: ▪ Internal/external audit results. ▪ Transaction monitoring logs and screening system outputs.
Accessibility and Format	▪ Records to be easily accessible for regulatory inspections.
Reporting Obligations	▪ Maintain copies of reports to regulatory bodies (e.g., FIU, JADIS).
Policy for Records Destruction	▪ Define secure destruction procedures after the retention period.

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

16. Oversight and Responsibility

A Money Laundering Reporting Officer (MLRO) is appointed to oversee and monitor our AML/CFT policies, maintain records, and serve as the primary point of contact for regulatory authorities and manages record-keeping responsibilities, including organizing, securing, and maintaining compliance-related records. Regular audits are conducted to assess and improve our practices, and roles are assigned to ensure accurate and timely regulatory reporting. This approach reflects our commitment to maintaining high standards of compliance and accountability.

Appendix 1. Country Risk Matrix

In assessing country risk associated with a customer relationship, Web3 Solutions S.r.l. will consider assessments and reports issued by credible independent sources, including the United Nations Sanctions Ordinance (UNSO), UNATMO, International Monetary Fund (IMF), World Bank, FATF, Transparency International, and similar organizations. Additionally, Web3 Solutions will consider its own experience and track record with customers from various jurisdictions, in compliance with MiCA regulations.

The following indications would normally lead Web3 Solutions S.r.l. to assess a country as high risk under MiCA regulations:

- Jurisdictions that do not or insufficiently apply the FATF Recommendations;
- Jurisdictions subject to sanctions, embargoes, or similar measures;
- Jurisdictions identified as having significant levels of corruption or other criminal activity.

Web3 Solutions S.r.l. does not operate in the following jurisdictions. This list is not exhaustive. Web3 Solutions will act reasonably in determining whether a transaction involves a prohibited jurisdiction:

Algeria, Argentina, Afghanistan, Bangladesh, Belarus, Benin, Bolivia, Burkina Faso, Burundi, Cambodia, Chad, China, Côte d'Ivoire, Congo (Democratic Republic of the), Crimea Region, Ecuador, Egypt, Eritrea, Ethiopia, Gabon, Indonesia, Iran (Islamic Republic of), Iraq, Jordan, Kosovo, Kuwait, Lebanon, Lesotho, Liberia, Libya, Malawi, Maldives, Mali, Morocco, Myanmar, Namibia, Nepal, Niger, North Macedonia, North Korea, Palau, Palestinian Territories, Pakistan, Qatar, Russia, Rwanda, Sierra Leone, Sri Lanka, Somalia, Syrian Arab Republic, Tanzania, Thailand, Togo, Tunisia, Turkey, Uganda, Ukraine, and Vietnam.

Some of the territories and countries classified as high risk are:

Barbados
Bulgaria
Burkina Faso
Cameroon
Croatia
Democratic People's Republic of Korea (DPRK)
Democratic Republic of the Congo
Gibraltar

Haiti
Iran
Jamaica
Mali
Mozambique
Myanmar
Nigeria
Philippines
Senegal
South Africa
South Sudan
Syria
Tanzania
Turkey
Uganda
United Arab Emirates
Vietnam
Yemen

Appendix 2. Customer Identification and Verification

Customer category	**Collect (at account opening or contract conclusion)** – upon accepting the Terms and Conditions and Terms of Use Of the Web3 Services	**Verify**
Natural Persons	. Full name a. National or foreign ID type and number b. Date of birth c. Nationality	**Proof of Identity:** Match of the full name, date of birth and the ID number. Valid ID document (passport, driving licence, residency card or national ID card) or a properly authorised data vendor. Where required or allowed by any law, national population register or national ID database may be utilised. All documents must be valid at the moment of the review. **Selfie:** match with photo on the ID.
Legal Entities	. Legal entity name a. Date and place of incorporation b. Business address c. Registration number or Tax/VAT number (depending on what is commonly used in	Copy of an ID or passport of every director and shareholder/UBO (who owns more than 25% of shares) and their proof of addresses; Proof of the company address. We accept the following address verification documents, issued within 90 days:

	the country, VAT number mandatory for EU) d. Contact phone number e. Website (optional) f. Account representative– the following details must be collected: ● Full name ● Date of birth ● Place of birth (country) ● Address ● National or foreign ID number and document type ● Nationality ● Phone number h. Directors, proxy-holders and UBO(s). Minimum information to be collected for all UBOs in excess of 25% ownership: ● Full name ● Date of birth ● Country of residence ● Nationality ● National or foreign ISD number and document type i. Industry category/subcategory	● bank statements - with transactions history - we accept digital bank statements too, just send us the original .pdf file (do note that sensitive information such as transactions details can be covered, transactions details); ● utility bills - electricity, water, waste management, fixed internet or phone bills (no mobile phone bills and insurance letters), etc. ● government issued letters - such as letters from government agencies, tax bills, etc. Certificate of the Registration of Incorporation/ registry extract; Memorandum of articles of Association / Constitution / By-Laws; Confirmation of an active status of the company (if it's not indicated in Registration Extract); Confirmation of the director (if it's not indicated in Registration Extract); Ownership structure: list of all Shareholders with the specified number of shares.

Appendix 3. Retailer or Customer Risk Matrix

The retailer or customer must be classified as High-Risk Customers if:

- there is 1 high risk factor present without corresponding mitigating factor

- there are 2 or more high risk factors present with or without corresponding mitigating factors.

High Risk Factors	Possible mitigating factors	Comment
Customer from a high risk country or associated with a high risk country	Customer makes payment in a small amount transaction	

Customer is a PEP	PEP is from a low risk country, low volume activity, no evident connection of Web3 activity to PEP's function	PEPs are always high risk
Retailer is from the high risk industry as per Appendix 4 of this Policy	Retailer has established a good track record with Web3, maintains low dispute, low refund levels, no complaints received, or retailer is a publicly listed company well recognized in the industry	Never make exceptions for charities, political fundraising, crowd-funding, gambling – they will always remain high risk retailers
Complex legal structures - trusts, foundations, nominal directors, holding companies that are used as holding vehicles, especially if combined with high risk jurisdictions	Retailer provided valid explanations of why they are organised in a certain way and there is evidence that they have appropriate substance and behave cooperatively. Established a good track record with Web3	Never dismiss a combination of a high risk country and a complex structure or a complex structure with a PEP affiliation. This factor is relevant for assessment of business partnerships and integrations.

Appendix 4. High Risk and Prohibited Industries

Prohibited Activities	High Risk Activities (need pre- approval)
• Autographed collectible (memorabilia) businesses • Diamond or Precious Metal Investment • Defence / Military Related • Hypnosis services • Mini-bonds • Multi-Level Marketing (MLM) • Nutraceuticals businesses • Psychic service • Shell Banks • Telemarketing Bureaus and Other Contact Centers • Unregulated financial or investment service • VoIP or telemarketing • Wine investment	• E-cigarettes • Products relating to dating services • Regulated Cannabis Industry • Agriculture / Farming • Adult content and services • Alcohol • Art Dealers • Boat Dealers • Business active in government procurement, i.e., those whose business is selling to government or state agencies • Cash-intensive business, including beauty parlours, newsagents, restaurants, bars, nightclubs, public houses, takeaways, and car washes • Chemical Manufacturing • Clothing Manufacturing • Construction and (large) infrastructure • Crowdfunding • Cyberlocker (an internet service that allows users to store and share files online) • Development and other types of assistance • Entertainment for minors • Estate Agency Business (EAB)

Web3 Solutions S.r.l
Company code: 13774000965
Address: Via del Lauro 9, 20121, Milan, Italy
email:info@lunu.io

	• Free port operator • Gaming / Casinos / Amusements • High value dealers, including luxury goods, precious metals, and precious stones • Hotels and accommodation in high risk countries • Language Schools • Letting Agency Business (LAB) • Loan Companies • Marinas • Mining and extraction • Negative option billing • Non EEA Charities or EEA Non Registered or Non Regulated Charities • NGO (non-governmental organisations) • Oil and Gas Pipeline and Related Structures Construction • Paper Manufacturing • Petroleum • Pharmaceutical • Plastics, Rubber, Metal Manufacturing • Precious Metal Production • Privatisation • Professional football • Property • Provision of public goods, utilities • Securities • Sugar • Tobacco • Travel / Travel Agencies / Tour Operators • Trust and Company Service Provider (TCSP) • Vehicle, Motorbikes, Plane, Jet, Boats- trade, maintenance, and repair • Waste management • Wealth management & private banking • Wholesale banking