Last updated on 10th October, 2025

Anti-Money Laundering and Counter-Terrorist Financing Policy

This Anti-Money Laundering and Counter-Terrorist Financing Policy (hereinafter – the "**Policy**") explains how STOCKENN LLC, a limited liability company incorporated under the laws of the State of Wyoming, United States of America, with its registered office at 30 N Gould St #47571, Sheridan, WY 82801 (hereinafter – the "**Company**"), implements measures aimed at preventing money laundering, terrorist financing, and other forms of financial crime.

We are committed to upholding unified global standards based on the most effective anti-money laundering ("**AML**") and counter-terrorist financing ("**CTF**") practices recognized in the United States and internationally.

To achieve this objective, the Company has adopted this Policy to prohibit and actively prevent the use of its services for money laundering, terrorist financing, or any activity that could facilitate such crimes.

Although the Company is not an obliged entity under U.S. AML legislation, we voluntarily implement robust internal measures to identify, assess, and mitigate potential risks. These include the application of Customer Due Diligence **("CDD")** procedures, such as Know Your Customer **("KYC")** verification, ongoing transaction monitoring, and other preventive controls consistent with best international practices.

Supplementary AML/CTF procedures, internal guidelines, and control mechanisms may be documented separately in support of this Policy. This Policy and all related procedures are subject to periodic review and timely updates to reflect the evolving risk environment and the Company's operational profile.

If you have any questions regarding this Policy, please contact us at: ***legal@stockenn.com***

1. Money laundering and terrorism financing overview

Money laundering refers to activities intended to conceal or disguise the unlawful origin of funds so that they appear to come from legitimate sources or represent lawful assets. The process generally unfolds in three stages:

- Placement – illicit proceeds are introduced into the financial system, for example by converting cash into monetary instruments (such as money orders or traveler's checks) or depositing it into accounts.
- Layering – the funds are transferred through multiple accounts or financial institutions in order to obscure their criminal source.
- Integration – the laundered funds are reintroduced into the economy, often through the purchase of lawful assets, investments, or businesses.

While direct cash deposits into securities accounts are uncommon, the securities industry presents unique vulnerabilities. It can both serve as a channel for laundering illicit funds from other sources and generate unlawful proceeds through fraudulent schemes such as insider trading, market manipulation, Ponzi schemes, cybercrime, or other investment-related misconduct.

Terrorist financing does not always involve criminal proceeds. Instead, it often seeks to obscure the origin or intended use of funds, which may themselves come from lawful sources. Unlike traditional criminal organizations, terrorist financiers frequently rely on legitimate income, including support from foreign governments, business operations, employment, or charitable contributions.

Although the motivations of money launderers and terrorist financiers differ, the methods employed can be similar, particularly in moving and disguising funds. Importantly, terrorist operations often require relatively modest amounts of money, with transactions that may appear straightforward and unremarkable.

Our anti-money laundering policies, procedures, and internal controls are established to maintain compliance with all applicable regulations. These measures are subject to regular review and ongoing updates to ensure they remain effective and appropriate in light of evolving regulatory requirements and business practices.

2. Client Verification Flow

To ensure proportional and risk-based compliance with AML and CTF standards, the Company applies a tiered verification process depending on the nature and value of the user's transactions.

All general information on the Platform is publicly accessible and may be viewed without registration. However, prior to being allowed to purchase DAO Tokens or conduct any financial transactions, every user must complete an User identification procedure through the Sumsub Compliance System, by submitting all required identification documents and information via the secure Sumsub interface.

The Company will assess and verify the user's identity, the purpose of the relationship before granting transaction access. Customer Due Diligence measures may be applied where risk indicators require additional scrutiny.

This includes verifying the user's identity, establishing the purpose of the relationship, and assessing the legitimacy and origin of funds. The scope and depth of verification are determined by the Company in accordance with its internal risk assessment procedures.

3. User identification

The initial collection of user information is one of the primary safeguards against the risk of the Company's services being misused for money laundering or terrorist financing.

This process ensures that the Company maintains awareness of who is using its Platform and can apply risk-based measures proportionate to the user's activity.

The Company collects and maintains basic information about each user connecting a wallet or interacting with the Platform.

This data is used to establish a user profile, assess potential risks, and ensure that the Company's services are not accessed by prohibited or high-risk individuals or entities.

Compliance with AML, CTF, and sanctions requirements is a key priority for the Company's management. Therefore, all user information is collected, processed, and stored in accordance with applicable laws, using secure internal procedures that guarantee the accuracy, integrity, and confidentiality of the data.

If, during the course of information collection or review, the Company:

- identifies or suspects that a user may be involved in money laundering, terrorist financing, or other unlawful activity;
- fails to receive sufficient cooperation or information to assess the user's profile; or
- determines that continuing the relationship would pose an unacceptable compliance risk,

the Company may:

- restrict, suspend, or terminate the user's access to its services; and
- escalate the case internally for further assessment and reporting to the Compliance function or senior management, as appropriate.

Before providing any services, the Company collects the following information (as applicable) from each User who connects a wallet to the platform:

- Full name;
- Date of birth;
- Copy of passport or ID;
- Email address;
- Country of residence;
- Phone number;
- Physical address, which may include:
    - a residential or business street address (for individuals);
    - an Army Post Office (**APO**) or Fleet Post Office (**FPO**) number, or the residential or business address of a next of kin or contact person (where the user has no fixed residential or business address);

4. Customer due diligence

CDD forms a fundamental part of our framework to mitigate the risks of money laundering, terrorist financing, and other illicit conduct. The Company's process is designed to conduct this due diligence post-factum, meaning after the business relationship with a user has been established. The Company initiates the

CDD process not for every user, but when specific triggers, as outlined in Section 4.1, are met.

To facilitate this process, each user is required to provide a minimum set of information during registration. This initial data collection is a prerequisite for the subsequent due diligence checks.

Following the establishment of the business relationship, the Company will use the provided information to perform comprehensive screening. Users will be checked against reliable databases and sources relevant to anti-money laundering and counter-terrorist financing to assess their potential risk exposure. This allows the Company to accurately identify and verify users in line with the requirements of the CDD Rule.

Based on this post-factum verification, the Company will analyze the nature and purpose of the business relationship to establish a risk profile for each user. This profile informs our ongoing monitoring, which includes detecting and reporting suspicious activity, as well as updating and maintaining user data using a risk-based approach.

4.1. Customer Due Diligence

CDD involves a structured set of actions aimed at confirming the user`s identity, understanding the nature of the relationship, and assessing potential risks. The core steps are:

1. The Company must collect and record essential details to establish who the user is.
2. The identity of the user must be confirmed through independent and trustworthy data, documents, or information. This step ensures that the details provided are accurate and reduces the risk of impersonation or fraudulent representation.
3. The Company will establish the reason why a user wishes to open or maintain a business relationship, or why a one-off transaction is being carried out.
4. To better evaluate the user, the Company will collect relevant background information and create a risk profile, which helps in spotting unusual or suspicious behavior. This assessment may include:
    - the individual’s occupation or employment;
    - the type and scope of the user's business activities;
    - assets currently held or managed (including trusts or holding entities);
    - the expected level and type of activity throughout the relationship;
    - the origin of funds (e.g., salary, business revenues, investments, inheritances, asset sales);
    - the source and overall level of wealth, particularly in high-risk cases;
    - justification for complex ownership structures;
    - jurisdictions the user is connected with;

    - criminal background or known associations with criminal groups;
    - whether the person qualifies as a Politically Exposed Person (**PEP**).

For this purpose the Company may also require documentary evidence such as:

- pay slips or employment confirmation letters;
- bank statements;
- business documentation (websites, brochures, business plans, financial forecasts, trade licenses);
- copies of contracts or draft agreements;
- audited financial statements;
- inheritance records, bills of sale, trust deeds or similar proof of wealth;
- results from business databases, regulatory registers, media checks, or international screening systems.

The Company will carry out standard due diligence in the following situations:

- whenever there is suspicion of money laundering or terrorist financing, regardless of exemptions or thresholds;
- in cases where the relationship or transaction presents elevated risks;
- when previously obtained identification data appears insufficient or unreliable.

5. Ongoing Monitoring

Ongoing monitoring refers to the continuous process of reviewing, updating, and enriching user identification data for AML/CFT compliance purposes. Its objective is to ensure that all information remains accurate, complete, and reflective of the user's current circumstances and risk profile.

Regular monitoring provides several key benefits:

- a more accurate and dynamic assessment of risk based on up-to-date information;
- sustained compliance with applicable AML/CFT regulations;
- complete and relevant user data to ensure appropriate service provision.

The Company conducts ongoing monitoring to identify and report suspicious transactions and to maintain current and accurate user information, including beneficial ownership details for legal entity users.

User activity is assessed against the user's risk profile to detect transactions or behaviors that deviate from expected patterns. When such deviations occur, the Company must determine whether the user's circumstances or risk level have changed.

All data and documents collected during the due diligence process must be reviewed and kept up to date through regular monitoring, particularly for users classified as higher risk.

The Company will review user information when specific events occur, such as:

- a user establishing a new relationship with the Company;

- a user changing their geographic location ;
- a user being included in a sanctions list, or associated with criminal activity;
- identification of unusual or suspicious transactions or behaviors during transaction monitoring.

6. Transaction Monitoring

The Company maintains continuous monitoring of transactions to detect unusual, suspicious, or potentially illicit activity in connection with money laundering, terrorist financing, fraud, or the use of proceeds of crime.

All incoming and outgoing crypto-asset transactions processed through the Platform are automatically and/or manually screened using specialized blockchain analytics tools and independent databases. These tools allow the Company to assess the source, counterparties, and risk level associated with each transaction.

The monitoring process includes, among others:

- tracing the origin and movement of crypto-assets on the blockchain;
- screening wallet addresses against sanctions lists, watchlists, and high-risk entity databases;
- identifying exposure to illicit activities, including darknet markets, ransomware, scams, or mixing services;
- reviewing the transaction value and frequency against the user's established risk profile.

If, based on the Company's assessment, any crypto-assets are identified as originating from or linked to illicit or high-risk sources, the Company reserves the right to:

- reject the transaction or suspend its processing;
- return the crypto-assets to the sender's wallet, after deducting applicable network or service fees; and
- report the incident to the Compliance function or relevant authorities where required by law.

Such actions are taken at the Company's sole discretion and form part of its commitment to maintaining a secure and transparent environment in accordance with international AML/CTF standards.

The Company does not assume responsibility for any losses or delays arising from the return of assets that are deemed high-risk or non-compliant under this Policy.

7. Unacceptable users

The following categories of users are strictly prohibited from accessing or using the Company's services.

The Company shall not establish or maintain a relationship with any user who:

- fails or refuses to provide the information or documents required for identity verification, without a valid justification;

- originates from, or is connected to, a jurisdiction that is banned under the Company's internal policies or subject to international sanctions;
- has been identified as a person or entity subject to international sanctions, including those issued under:
    - the International Sanctions Act;
    - United Nations (UN) Sanctions;
    - European Union (EU) Sanctions;
    - Sanctions administered by the UK Office of Financial Sanctions Implementation (OFSI);
    - Sanctions administered by the U.S. Office of Foreign Assets Control (OFAC);
- is reasonably suspected of being involved in money laundering, terrorist financing, or other criminal activity;
- is otherwise assessed by the Company as posing an unacceptable or disproportionate risk in accordance with applicable AML/CFT laws and internal risk assessment criteria.

The Company does not accept users (natural or legal persons) originating from or residing in the following countries or regions:

Afghanistan, Barbados, Belarus, Burma (Myanmar), Burkina Faso, Burundi, Cambodia, China, Central African Republic, Cuba, Democratic Republic of the Congo, Democratic People's Republic of Korea (North Korea), Ethiopia, Guinea, Guinea-Bissau, Haiti, Iran, Iraq, Jamaica, Jordan, Lebanon, Libya, Mali, Nicaragua, Pakistan, Panama, Philippines, Russia, Senegal, Somalia, South Sudan, Sudan, Syria, Tunisia, Uganda, Venezuela, Yemen, Zimbabwe, and the following regions of Ukraine: Crimea, Donetsk, and Luhansk.

Users from jurisdictions where the Company's services would require a specific authorization, license, or registration will not be accepted unless the Company holds such authorization or license in the respective jurisdiction.

8. Training obligations

The Company is committed to ensuring that all employees, management, and Senior Management members possess a sound understanding of AML/CFT requirements and are capable of identifying and mitigating money laundering, terrorist financing, and proliferation financing risks. To achieve this, the Company shall:

1. Provide comprehensive and risk-based training in line with applicable regulatory requirements, covering relevant AML/CFT concepts, controls, and procedures;
2. Implement effective mechanisms to assess employees' understanding and awareness of the training materials provided.

Training is mandatory for:

- Members of the Senior Management;

- Employees directly involved in AML/CFT-related tasks and compliance activities;
- Employees of third parties performing AML/CFT or related functions under outsourcing arrangements.

While training focuses primarily on key personnel, the Company recognizes that AML/CFT awareness must extend to all employees to maintain a culture of compliance across the organization.

Training must be conducted at least once per year and additionally whenever there are significant updates to AML/CFT legislation, internal procedures, or risk typologies.

Interactive training methods are encouraged to ensure active participation and deeper understanding of the subject matter.

All training sessions must be properly documented in accordance with the Company's record-keeping requirements. Records should include:

- the date of the training session;
- topics covered;
- names and positions of participants;
- names of trainers or facilitators; and
- confirmation of attendance and completion.

9. Changes to this policy

The Company reserves the right to revise, amend, or update this Policy at its sole discretion to reflect changes in regulatory requirements, business operations, or industry best practices. The effective date of the most recent revision will always be indicated at the top of this document.

When material amendments are made, the Company will notify users in a manner appropriate to the nature and significance of the changes. Where required by applicable law, the Company will obtain user consent prior to implementing substantial modifications.

If a user does not agree with the updated version of this Policy, the user must discontinue the use of the Company's services.

For any questions, requests, or clarifications regarding this Policy, users may contact the Company via email at legal@stockenn.com.