

Crypto Risk Policy for Silkwave Tech BV

Introduction

This Risk and Know Your Customer (KYC) policy outlines the procedures and standards that Silkwave Tech BV ("the Company") will implement to ensure compliance with Anti-Money Laundering (AML) regulations, Counter-Terrorism Financing (CTF) guidelines, and other regulatory obligations concerning the identification and verification of customers. This policy addresses both cryptocurrency deposits and withdrawals, ensuring the security, integrity, and regulatory compliance of all transactions on the platform.

Purpose

The purpose of this policy is to:

- Prevent money laundering, terrorist financing, and other illegal activities.
- Verify the identity of users making cryptocurrency deposits and withdrawals.
- Ensure compliance with international regulatory standards and best practices.
- Protect the integrity of the Company's operations and safeguard its customers.

Scope

This policy applies to all customers engaging in cryptocurrency transactions, including deposits, withdrawals, and transfers, on the Company's platform. It governs how the Company collects, verifies, and maintains customer data to mitigate risks associated with illegal activities.

The company has implemented a system that will detect those individuals that, based on the customer profile, are deemed to fall outside the 'Norm', and such Customers will be outrightly refused or reported if deemed necessary. Criminals are always developing new techniques, so this list can never be exhaustive. We are to remain vigilant, and if new typologies are identified are to be raised with the MLRO.

1. Customer Identification Procedures (CIP)

1.1 KYC Requirements

Before customers can make cryptocurrency deposits, they must undergo KYC verification. The verification process will involve the collection of:

- **Full name.**
- **Date of birth.**
- **Residential address**

Upon withdrawal customers must provide a full KYC verification which will validate their previous basic details

- **Government-issued identification (passport, national ID card, driver's licence).**
- **Selfie or video confirmation for identity validation** (live selfie or verification against submitted ID).

The Company reserves the right to request additional documentation, such as proof of address (utility bill, bank statement) or a second form of ID, if necessary.

1.2 Verification Process

- **Automated Verification:** The Company will use third-party KYC verification providers for real-time verification of submitted documents and biometric data.
 - **Manual Review:** Any discrepancies or red flags raised during automated checks will trigger a manual review by the Company's compliance team.
 - **Re-verification:** Customers must re-submit their documents if they change their name, address, or when the current KYC documentation expires.
-

2. Cryptocurrency Transaction Monitoring

2.1 Wallet Screening

The Customer will be questioned on the type of wallet being used, and the hash of the wallet will be held and verified against a third-party provider:

- Multi-signature wallets are to be verified, and each individual holding keys shall be treated as a beneficial owner of the account and will need to be verified.
- Those custodial wallets which are not subject to any verification shall be assessed, and if they are likely to pose a high risk of ML/FT will be placed on a list of providers for whom the wallet will be black listed. All wallets depending on the activity limits and thresholds, shall be scrutinised for ownership and illicit activity.
- If the Customer indicates a wallet that is not held on his behalf, such will be scrutinised.

The wallets are to be screened:

- When the Customer is depositing funds; or
- When the Customer is transferring funds out of the system.

Screening of wallets is conducted using blockchain analysis and helps to understand where the funds are received and sent to. This is to ensure further that funds are not remitted to wallets which have links to financial crime and will ensure complete plotting of the transaction and that when funds are transferred out of the system they are processed to the same wallet used to deposit (closing the loop).

If there is an alert on any wallet it will be reported immediately to the MLRO.

Note: Each time a Customer deposits from a new wallet the above is conducted on each wallet added; Customer shall be questioned on the type of wallet & hash of the wallet shall be verified against wallet screening. If the Customer is using multiple wallets this is a potential ML/FT concern and will be taken into account in the CRA and raised to the appropriate authorities if required.

2.1.1 Blacklisted Wallets (non-CAP)

The company takes a heavy stance on blacklisted wallets, whether blacklisted or sanctioned by Authorities or blacklisted by the company. The company will use a system which detects any transaction emanating from or being sent to blacklisted wallets. If such a transaction is detected, the payment will be frozen, and funds will not be transferred.

2.1.2 The Use of Privacy Coins

The use of privacy coins that may render the Customer anonymous are strictly prohibited. The wallets the Customer is to deposit are to be screened upon the inception of the account using software that will generate a report which will influence the Customer's risk score. The company shall adopt a clear-cut approach meaning that if a high-risk wallet is identified, the wallet and the Customer will not be allowed on the platform and shall be banned from further interaction.

The company is currently looking to obtain a third-party verification provider which shall be part of the onboarding process at deposit stage. All tokens offered on the platform will have to go through a financial instrument test, along with an internal audit of the token for AML/CFT purposes.

2.2 Transaction Screening

All cryptocurrency transactions will be monitored and analysed through blockchain analysis tools that can detect:

- Use of **mixers/tumblers** to obscure the source of funds.
- Connections to **dark web** marketplaces or other illegal activities.
- Transactions originating from **high-risk countries** or regions identified by the Financial Action Task Force (FATF).

2.3 Flagging and Reporting Suspicious Activity

- Any suspicious or unusually large cryptocurrency transactions will be flagged for review by the compliance team.
- Transactions that are potentially linked to money laundering or terrorist financing activities will be reported to the relevant authorities in accordance with AML/CTF regulations.

2.3 Transaction Limits

The Company may impose transaction limits on cryptocurrency deposits and withdrawals depending on the customer's risk profile. Higher limits may be granted only after thorough KYC and additional Enhanced Due Diligence (EDD).

3. Enhanced Due Diligence (EDD)

3.1 High-Risk Customers

Customers identified as high-risk will undergo Enhanced Due Diligence, which includes:

- Additional identity verification (e.g., video KYC or third-party biometric checks).
- Source of wealth or source of funds verification for larger transactions.
- Continuous monitoring of account activity to detect any changes in risk levels.

3.2 EDD Triggers

EDD will be triggered in the following circumstances:

- Transactions over a certain threshold (set internally by the Company based on risk).
 - Customers from jurisdictions with high levels of financial crime or inadequate AML controls.
 - Involvement of politically exposed persons (PEPs) or sanctioned individuals.
-

4. Data Collection, Storage, and Security

4.1 Data Collection

All customer information collected for KYC purposes will be securely stored and maintained in compliance with applicable data protection laws, such as GDPR.

4.2 Data Retention

Customer KYC data will be retained for a minimum of five years after the business relationship has ended or in accordance with local regulatory requirements, whichever is longer.

4.3 Data Security

The Company will implement strong encryption protocols and other industry-standard cybersecurity measures to protect customer data from unauthorized access or breaches.

5. Regulatory Compliance

5.1 AML and CTF Laws

The Company will adhere to all local and international AML and CTF laws and regulations. Regular audits and reviews will be conducted to ensure compliance.

5.2 Reporting Obligations

The Company will report any suspicious activity, including large or unusual cryptocurrency transactions, to the relevant authorities (e.g., Financial Intelligence Units, regulators) as required by law.

5.3 Training and Awareness

All employees involved in KYC, customer service, and cryptocurrency transactions will receive ongoing training to stay up-to-date on regulatory changes and best practices in AML/CTF compliance.

6. Risk Management and Ongoing Monitoring

6.1 Risk-Based Approach

The Company will adopt a risk-based approach to KYC and customer verification, applying stricter controls and due diligence to high-risk customers, transactions, and jurisdictions.

6.2 Ongoing Monitoring

The Company will conduct continuous monitoring of all customer transactions, particularly those involving cryptocurrency, and will flag unusual patterns or behaviors for further review. Customers will also be subject to periodic re-verification to ensure that their KYC information remains accurate and up-to-date.

7. Crypto Withdrawal Policy

7.1 KYC Requirements for Withdrawals

Before initiating cryptocurrency withdrawals, customers must have completed KYC verification as outlined above. Withdrawals will not be processed for accounts that have not undergone the necessary KYC checks.

7.2 Withdrawal Screening

All crypto withdrawal requests will be subject to screening, including:

- **Transaction Monitoring:** The Company will analyse the destination wallet address for any links to high-risk activities, such as connections to darknet markets, mixers, or previously flagged illicit transactions.
- **Suspicious Activity:** Large or unusual withdrawals will be flagged for manual review by the compliance team. Withdrawals to wallets in high-risk jurisdictions or using potentially anonymous wallet services may trigger additional scrutiny.

7.3 Withdrawal Limits

- **Tiered Withdrawal Limits:** The Company may apply different withdrawal limits based on the customer's KYC tier, risk profile, and transaction history.
 - **Unverified Accounts:** No withdrawals permitted until KYC is completed.
 - **Basic KYC Tier:** Withdrawals allowed up to a set limit per day/month.
 - **High-Volume Accounts:** Subject to additional EDD and may qualify for higher withdrawal limits.

7.4 Source of Funds Verification

For withdrawals over a set threshold, the Company may request additional documentation to verify the source of the cryptocurrency funds (e.g., documentation showing how the cryptocurrency was acquired, trading history, or a declaration of income).

7.5 Delayed or Blocked Withdrawals

The Company reserves the right to delay or block cryptocurrency withdrawals under the following circumstances:

- Suspicious activity is detected in the account or the transaction.
- The withdrawal request exceeds set limits and requires further verification.
- Regulatory or legal obligations require the freezing of funds.

Customers will be notified if their withdrawal is delayed or requires additional information for processing.

7.6 Withdrawal Fees

Cryptocurrency withdrawals are subject to standard network fees, as well as any additional processing fees that may be applied by the Company. Fees will be disclosed prior to confirming the withdrawal.

8. Customer Communication and Support

8.1 KYC and Withdrawal Transparency

The Company will clearly communicate KYC and withdrawal requirements to all customers during account registration, deposit, and withdrawal processes. Customers will be informed of the steps involved in verification, withdrawal limits, and any documents required.

8.2 Support Channels

The Company will provide 24/7 customer support to assist users with any issues related to KYC verification, withdrawal requests, or transaction inquiries.

9. Policy Updates and Reviews

This KYC and Crypto Withdrawal policy will be reviewed and updated regularly, at least annually, to ensure it remains in line with current laws, regulations, and industry best practices. Any significant changes to the policy will be communicated to customers promptly.

10. Non-Compliance

Failure to comply with KYC verification or the withdrawal policy will result in:

- **Inability** to withdraw cryptocurrency from the platform.
 - Potential **account suspension** or **closure**.
 - Reporting to relevant authorities in cases of suspected illegal activities.
-

Conclusion

The Company is committed to maintaining a secure and compliant iGaming environment by adhering to the highest KYC, AML, and CTF standards. This policy ensures that we protect our platform from illicit activities while safeguarding our customers' information and funds during both deposits and withdrawals.