Husher

Anti-Money Laundering Policy

Last Updated: 17 November 2025

This Anti-Money Laundering Policy ("AML Policy" or "Policy") outlines the provisions and procedures through which HUSH Technology Inc. ("We", "Us", or "Our") proactively combats unlawful activities and safeguards our Services from being utilized for laundering funds originating from illegal sources, while ensuring compliance with applicable laws and regulations related to Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements.

1. Our Commitment to AML Compliance

We are committed to promoting security for our partners and users by actively protecting them from fraudulent activity and maintaining the highest levels of financial integrity. Our team has developed a comprehensive framework of AML Systems and Procedures (collectively, "AML Measures") to detect, prevent, and report suspicious activities.

1.1 AML System

Our AML System is an advanced algorithmic risk evaluation and transaction monitoring solution that operates using:

- Risk-Based Approach: Transactions are evaluated based on calculated risk levels
- Internal Blacklisting: Known suspicious addresses and entities are flagged
- Volume-Oriented Dynamic Limits: Exchange limits adjust based on risk factors
- Multi-Factor Analysis: Numerous checks consider various criteria, factors, and weighted parameters

Risk Score Calculation: For every transaction, our System produces a final Risk Score expressed as a percentage. This system has been developed and refined over years to demonstrate exceptional performance in detecting suspicious transactions and user activities.

Confidentiality: We cannot disclose the specific criteria and parameters contributing to risk scores, as this would compromise the effectiveness of our system and enable circumvention.

Processing Flow: When you initiate an order and your deposit is received, our System calculates the Risk Score before processing. If the score surpasses accepted risk levels, AML Procedures may be triggered.

1.2 AML Procedures

Our AML Procedures encompass a series of actions designed to verify the legitimacy of funds and ensure users adhere to all legal compliance requirements in accordance with applicable laws and our Terms of Service.

When triggered, the following actions may occur:

- Transaction Hold: Your transaction is temporarily paused for review
- KYC Verification: Identity verification requirements

- Source of Funds (SOF) Inquiries: Documentation proving the origin of your funds
- Manual Review: Human evaluation of the transaction and associated account
- Transaction Freezing: Extended hold pending investigation
- Account Restrictions: Limitation or suspension of account access
- Transaction Reporting: Notification to relevant authorities as required by law

The specific procedures applied depend on the circumstances and risk level of each case.

2. User Acceptance and Warranties

By using our Services, you warrant and agree to:

- Acceptance of AML Procedures: You acknowledge that AML Procedures may be applied to your transactions
- Cooperation: You will promptly provide requested information and documents
- Compliance: You understand that both Husher and our partner Exchange Service Providers (ESPs) may request documentation to identify you, prove the source of funds, and ascertain compliance with our Terms of Service and applicable laws

2.1 Ongoing AML Requirements

We reserve the right to:

- Conduct AML Procedures on an ongoing basis at any time
- Request verification proactively when circumstances change (e.g., updated identification documents, change in transaction patterns)
- Apply procedures when user activity is considered suspicious or high-risk, whether identified through our AML System or at our sole discretion
- Request up-to-date documents from any user, even if they have successfully passed AML Procedures in the past Important: Previous successful verification does not exempt you from future AML Procedures.

3. Required Documentation

During AML Procedure enforcement, you may be requested to provide:

3.1 Identity Verification (KYC)

- Government-Issued ID: A high-quality photo of your valid passport, driver's license, or national identity card
- Selfie Photo: A clear photo of yourself to verify it matches your identification document
- Liveness Checks: Real-time verification requiring you to follow random instructions (e.g., turn your head, blink, hold up a specific document) to ensure the KYC process is conducted live and authentically

3.2 Source of Funds (SOF)

Documentation proving your funds originate from legal sources, which may include:

- Bank statements showing the origin of deposited cryptocurrency

- Proof of income or employment
- Proof of cryptocurrency purchase receipts
- Exchange account statements
- Any other documentation deemed necessary to verify fund legitimacy

3.3 Additional Documentation

We reserve the right to request any additional documentation necessary to ascertain:

- Your funds originate from legal sources
- Your compliance with our Terms of Service
- Your compliance with applicable laws in your jurisdiction

Response Timeframe: You must provide requested documentation within a reasonable timeframe specified in our request (typically 5-14 days). Failure to comply may result in transaction refusal, account restrictions, or fund freezing.

4. Evaluation Process

4.1 Conducting Evaluation

Third-Party Verification Partners: We may appoint certified third-party service providers to:

- Review submitted documentation
- Ascertain the authenticity of provided documents
- Carry out identity verification on our behalf
- Conduct liveness checks and biometric analysis

All third-party providers are required to comply with our Privacy Policy and applicable data protection laws to guarantee the security and confidentiality of your personal information.

Evaluation Methods: Once we receive requested documentation, evaluation is conducted:

- Programmatically: Using AI-powered verification software through our third-party partners
- Manually: Human review by our compliance team
- Hybrid Approach: Combination of both methods depending on the case and AML Procedures enforced

4.2 Data Storage and Security

Secure Storage: All documentation you provide is securely stored according to applicable data protection laws and for as long as required by law (typically up to 5 years).

Confidentiality: Documents are never disclosed to unauthorized parties. Exceptions include:

- Competent governmental authorities
- Law enforcement agencies
- Regulatory bodies
- Investigative authorities

Disclosure occurs only upon official request as provisioned in our Privacy Policy.

4.3 Positive Evaluation Result

If your documents and verification procedure are found to be:

- Valid and authentic
- In line with our Terms of Service
- Compliant with applicable laws

Then: Verification is finalized successfully, and your transaction is processed automatically.

4.4 Negative Evaluation Result

A negative result occurs when:

- You fail to satisfy AML Procedure requests
- Your details or account(s) appear on blacklists or sanction lists
- You violate our Customer Acceptance Policy or Terms of Service
- You fail to provide requested documentation within the specified timeframe
- Provided documents cannot be deemed authentic or are insufficient
- Documents are fraudulent, altered, or belong to someone else

Consequences of negative results:

- Service Refusal: We reserve the right to stop providing Services to you
- Transaction Not Processed: Your exchange will not be completed
- Account Restriction: Your account may be limited or suspended
- Refund with Deductions: Deposited amount is refunded minus compensatory charges for any damages Husher may suffer (including but not limited to investigation costs, third-party verification fees, and administrative expenses)

4.5 Severe Cases: Non-Cooperation and Suspected Illegal Activity

When the following conditions exist:

- You are not cooperating with our AML Procedures
- You have failed to respond to previous AML requests
- The transaction is suspected of being related to illegal activities
- Patterns indicate money laundering, terrorism financing, or other criminal activity
- Your account or addresses are linked to known illegal entities or activities

We reserve the right to:

- Freeze the Transaction: Indefinitely hold funds pending investigation
- Cold Storage Transfer: Move frozen funds to a secure cold storage wallet for the period necessary to complete investigation
- Extended Investigation: Conduct thorough review which may take weeks or months
- Report to Authorities: Submit the case to relevant law enforcement, regulatory bodies, or financial intelligence units for investigation and guidance
- Permanent Account Ban: Restrict your access to our Services indefinitely

Important: In cases of suspected illegal activity, refunds may be withheld pending authority guidance, and we will fully cooperate with law enforcement investigations.

5. Red Flags and Suspicious Activity

We monitor for suspicious activity indicators, including but not limited to:

- Transaction Patterns: Structuring transactions to avoid thresholds, rapid deposits and withdrawals, unusual transaction timing
- Address Analysis: Use of mixers/tumblers, connections to darknet markets, addresses on sanction lists, frequent address changes
- Behavioral Red Flags: Providing false information, refusing to provide requested documentation, inconsistent transaction explanations, using stolen or fake identity documents High-Risk Jurisdictions: Transactions involving sanctioned countries or high-risk jurisdictions
- Volume Anomalies: Sudden significant increases in transaction volume or value

If we detect suspicious activity, AML Procedures will be triggered immediately.

6. Prohibited Activities

You are strictly prohibited from using our Services for:

- Money laundering or terrorist financing
- Fraud, corruption, or embezzlement
- Purchase or sale of illegal goods or services (drugs, weapons, stolen goods, etc.)
- Human trafficking, organ trafficking, or any form of illegal trafficking
- Proceeds from ransomware, hacking, or cybercrime
- Sanctions evasion or transactions with sanctioned entities
- Tax evasion or unreported income laundering
- Any other illegal activity under applicable laws

If we detect prohibited activity, we will refuse service, freeze funds, report to authorities, and cooperate fully with investigations.

7. Cooperation with Authorities

Husher fully cooperates with:

- Law enforcement agencies
- Financial intelligence units (FIUs)
- Regulatory authorities
- International organizations combating financial crime

We will:

- Respond promptly to official information requests
- Provide transaction data, user information, and documentation as legally required
- Report suspicious activity in accordance with legal obligations
- Maintain confidentiality of ongoing investigations

Husher

8. Limitation of Liability

Our Commitment: Husher takes all necessary actions and measures, uses best available practices, and follows the most efficient course of action to prevent fraudulent and illegal activity.

Service Refusal: We refuse to develop business relationships or provide Services to any individual or entity suspected of:

- Money laundering
- Terrorism financing
- Corruption or fraud
- Illegal transfer of assets
- Drug, human, or organ trafficking
- Any other illegal trafficking or criminal activity

Liability Disclaimer: In no event shall Husher, our owners, directors, officers, employees, or agents be liable or responsible if our Services are used by any user for illegal activity or in violation of applicable law, even if the associated user has passed an AML Procedure.

System Limitations: We exempt liability for any deficiency or error that may arise from human or system error in:

- Identifying suspicious transactions or user activity
- Proactively denying Services to users suspected of or associated with illegal activity
- False negatives in risk assessment

Best Efforts: While we employ sophisticated systems and procedures, no AML system is perfect. We operate on a best-efforts basis and continuously improve our detection capabilities.

9. Updates to This Policy

This AML Policy may be updated periodically to reflect:

- Changes in applicable laws and regulations
- Improvements to our AML Systems and Procedures
- Evolving best practices in financial crime prevention
- Emerging threats and risk factors

Your Responsibility: Regularly review this Policy to stay informed of changes. Continued use of our Services constitutes acceptance of the updated Policy.

Husher

10. Contact Us

If you have questions related to our AML Policy or need assistance with AML Procedures:

- Email: support@husher.io
- Website: https://husher.io
- Telegram Bot: https://t.me/HusherOfficialBot

For AML-related inquiries, please include "AML Inquiry" in your subject line for faster processing.

By using Husher's Services, you acknowledge that you have read, understood, and agree to comply with this Anti-Money Laundering Policy.

