Anti–Money Laundering (AML) Policy

Company: DMSX Token LLC
Registered Address: 8 The Green, STE B, 19901 Dover, Delaware, United States
Effective Date: 11th November 2025
Applies To: All employees, contractors, investor onboarding activities, and digital asset transactions through https://www.domus-x.io

1. Purpose and Regulatory Context

DMSX Token LLC ("**DomusX**," "**the Company**") maintains this Anti–Money Laundering and Counter-Terrorist Financing Policy ("**Policy**") to ensure compliance with:

- the **Bank Secrecy Act (BSA)** (31 U.S.C. § 5311 et seq.);
- the **USA PATRIOT Act of 2001**;
- **FinCEN** regulations (31 C.F.R. Chapter X);
- **OFAC** sanctions programs; and
- relevant **FATF Recommendations** on virtual assets.

The objective is to prevent the Company and its digital-token platform from being used for money laundering, terrorist financing, fraud, tax evasion, or other financial crimes.
This Policy supports compliance with U.S. law, Delaware LLC requirements, and securities exemptions under **Regulation D (Rule 506(c))** and **Regulation S** of the Securities Act of 1933.

2. Scope and Applicability

2.1 This Policy applies to:

- all employees, officers, contractors, and consultants of DomusX;
- any affiliate, subsidiary, or joint-venture entity engaged in token issuance or investor onboarding;
- third-party service providers performing **KYC**, **AML**, **custody**, or **payment** services; and
- all investors, subscribers, and beneficial owners participating in the **DMSX Token Offering**.

2.2 It governs every stage of the token lifecycle — subscription, payment, issuance, transfer, and redemption — and extends to both U.S. and offshore (Reg S) participants.

3. Definitions

For purposes of this Policy:

- **Money Laundering:** The process of concealing the origin of proceeds derived from criminal activity.

- **Terrorist Financing:** The collection or provision of funds intended to be used to carry out terrorist acts.
- **Beneficial Owner:** The natural person(s) who ultimately owns or controls an investor or on whose behalf a transaction is conducted.
- **Politically Exposed Person (PEP):** An individual who is or has been entrusted with prominent public functions, as well as their immediate family and close associates.
- **Sanctioned Person:** Any individual or entity listed by **OFAC**, **UN**, **EU**, or **UK HMT** sanctions regimes.
- **Customer Due Diligence (CDD):** Processes used to verify the identity of investors and assess money-laundering risk.
- **Enhanced Due Diligence (EDD):** Additional verification for higher-risk investors or transactions.
- **Suspicious Activity:** Any behavior that appears inconsistent with the known profile or legitimate business of the investor.

4. AML Governance and Responsibilities

4.1 **Board Oversight:** The Board of Managers or equivalent governing body approves this Policy and oversees its implementation.

4.2 **AML Compliance Officer (AMLCO):** The Company designates an experienced officer responsible for:

- developing and maintaining the AML program;
- monitoring transactions and filing suspicious activity reports where required;
- serving as the contact point for FinCEN and OFAC; and
- reporting quarterly to management on compliance metrics and findings.

4.3 **Employee Responsibility:** Every employee must understand and comply with this Policy, complete mandatory training, and immediately report any suspicious activity to the AMLCO.

4.4 **Independence:** The AMLCO acts with full authority and autonomy, free from business or sales influence.

5. Customer Identification Program (CIP)

5.1 Before establishing any business relationship or accepting funds, DomusX must identify and verify each investor's true identity.

5.2 **Information Collected (Individuals):**

- full legal name, date of birth, nationality;
- residential address and email contact;
- government-issued photo identification;
- selfie or biometric verification (if required).

5.3 **Information Collected (Entities):**

- legal name, registration number, and jurisdiction;
- registered address and directors;
- ultimate beneficial owners (≥ 25 % ownership);
- corporate documents (e.g., certificate of formation, articles of organization).

5.4 **Verification Methods:** Electronic ID verification, video KYC, database cross-checks, and manual document review.

5.5 **Sanctions and Watch-List Screening:** All investors are screened against OFAC, UN, EU, UK HMT, and domestic terror lists prior to approval.

5.6 Records of verification and screening results must be kept for at least five years after the end of the relationship.

6. Customer Due Diligence (CDD) and Risk Profiling

6.1 The Company employs a risk-based approach to assess each investor according to:

- country of residence or registration;
- occupation or business activity;
- source of funds and wealth;
- transaction volume and pattern; and
- exposure to PEPs or sanctioned countries.

6.2 Each investor is assigned a risk rating (low, medium, high) that determines the depth of ongoing monitoring.

6.3 Higher-risk investors trigger Enhanced Due Diligence under Section 7.

6.4 Risk ratings are reviewed annually or upon any material change in circumstances.

7. Enhanced Due Diligence (EDD)

7.1 EDD applies where:

- the investor is a PEP or related to one;
- funds originate from high-risk or non-transparent jurisdictions;
- the investor's corporate structure is complex or involves offshore entities; or
- the subscription amount exceeds internal thresholds.

7.2 EDD may include:

- obtaining independent proof of source of funds and wealth;

- conducting open-source media searches for adverse information;
- requiring additional senior management approval; and
- ongoing review of transactions linked to the investor.

7.3 Where EDD cannot satisfactorily confirm legitimacy, the relationship shall not proceed or must be terminated.

8. Ongoing Monitoring and Screening

8.1 All transactions are monitored for consistency with the investor's profile.

8.2 Indicators of potential suspicious activity include (but are not limited to):

- repeated attempts to use multiple wallets or identities;
- transactions just below reporting thresholds;
- unexplained fund movements through high-risk jurisdictions; or
- refusal to provide additional information.

8.3 Automated systems generate alerts for review by the AMLCO.
All alerts must be documented with resolution outcomes.

8.4 Periodic rescreening against OFAC and PEP lists occurs at least quarterly or upon major list updates.

9. Recordkeeping and Retention

9.1 The Company maintains accurate and complete records of:

- identification documents and verification results;
- account files and transaction data;
- risk assessments, EDD findings, and internal approvals;
- communications with regulators or law enforcement; and
- suspicious-activity review logs.

9.2 Records are retained for a minimum of **five (5) years** after the termination of the relationship or completion of the transaction, whichever is later.

9.3 All records are stored securely in electronic form, with access restricted to authorized personnel and protected by encryption and audit logs.

10. Reporting of Suspicious Activity

10.1 Employees must promptly report any suspected money-laundering or terrorist-financing activity to the AMLCO.

10.2 The AMLCO reviews all reports and determines whether a **Suspicious Activity Report (SAR)** must be filed with **FinCEN** in accordance with 31 C.F.R. § 1022.320.

10.3 SARs must be filed within 30 days of initial detection of facts constituting suspicion and kept confidential.
Employees are prohibited from disclosing that a SAR has been filed ("tipping off").

10.4 The AMLCO maintains a register of all internal and external reports, including dates, decisions, and follow-up actions.

10.5 In cases of imminent threat or terrorist activity, law enforcement and OFAC shall be notified immediately before filing a SAR.

11. OFAC Sanctions Compliance

11.1 The Company fully complies with all economic and trade sanctions administered by the **U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC)** and other applicable regimes (United Nations, European Union, U.K. HMT).

11.2 All investors, counterparties, and related parties are screened before onboarding and periodically thereafter against:

- the OFAC **Specially Designated Nationals (SDN)** List;
- the **Sectoral Sanctions Identifications (SSI)** List; and
- other relevant government watchlists.

11.3 Any positive or potential match is immediately escalated to the AMLCO for review. If confirmed, the account or transaction will be frozen or rejected, and a blocking report will be filed with OFAC within ten (10) business days.

11.4 No business shall be conducted with, or for the benefit of, any sanctioned jurisdiction, entity, or person.

11.5 All OFAC screening logs, correspondence, and reports are maintained for a minimum of five years.

12. Training and Awareness

12.1 Every employee, director, and contractor must complete **initial AML training** upon onboarding and **annual refresher training** thereafter.

12.2 Training covers:

- money-laundering and terrorist-financing typologies;
- recognition of suspicious indicators;

- recordkeeping and reporting duties; and
- confidentiality and data-protection obligations.

12.3 Completion of training is mandatory; non-participation may result in disciplinary action.

12.4 The AMLCO documents attendance and test results and reviews content annually to ensure relevance to emerging risks and regulations.

13. Independent Audit and Program Review

13.1 An **independent audit** of the AML program is conducted at least once every twelve (12) months by qualified internal audit staff or an external compliance consultant.

13.2 The audit assesses:

- adequacy of policy design;
- operational effectiveness of KYC/CDD/EDD controls;
- quality and timeliness of SAR filings;
- employee knowledge and training; and
- overall risk-management framework.

13.3 Findings and recommendations are documented in a written report submitted to senior management and the Board.

13.4 Management must document corrective actions and implementation timelines.

14. Use of Third-Party Providers

14.1 DomusX engages third-party vendors for KYC/AML verification, custodial, and payment-processing services only after conducting due diligence to confirm their competence, licensing, and data-security standards.

14.2 All third-party relationships are governed by written contracts requiring:

- adherence to this Policy and all applicable AML/CTF laws;
- immediate reporting of suspicious activity;
- cooperation with audits and regulatory requests; and
- data-protection safeguards equivalent to DomusX’s internal standards.

14.3 The AMLCO maintains a register of approved vendors and reviews them annually for continued suitability.

15. Data Protection and Confidentiality

15.1 All personal and financial data obtained under this Policy are processed in accordance with the Company's **Privacy Policy** and relevant data-protection laws.

15.2 KYC and transaction records are encrypted and stored on secure servers located in the United States.

15.3 Access to sensitive data is restricted to authorized compliance personnel on a need-to-know basis and logged for audit.

15.4 Information obtained in connection with AML investigations or SAR filings is strictly confidential and must never be disclosed externally except to competent authorities as required by law.

16. Reporting to Senior Management and Board Oversight

16.1 The AMLCO provides **quarterly compliance reports** summarizing:

- number of new investors onboarded;
- alerts raised and resolved;
- SARs filed;
- sanctions hits; and
- any material control breaches.

16.2 Significant incidents, regulatory inquiries, or confirmed breaches must be reported to the Board of Managers immediately.

16.3 The Board reviews and approves this Policy annually and ensures adequate resources for its implementation.

17. Breaches and Disciplinary Action

17.1 Failure to comply with this Policy constitutes a disciplinary offense.

17.2 Depending on severity, sanctions may include written warning, suspension, termination, and, where applicable, referral to regulatory or law-enforcement authorities.

17.3 The Company enforces a **zero-tolerance** approach to willful non-compliance or concealment of suspicious activity.

17.4 Employees and contractors have a duty to cooperate fully in all internal or external AML investigations.

18. Review and Updates

18.1 This Policy is reviewed at least annually or sooner if:

- relevant legislation or regulation changes;
- FinCEN, OFAC, or SEC issue new guidance; or
- internal audits identify areas for improvement.

18.2 All amendments are approved by senior management, recorded in the version-control register, and communicated to staff.

18.3 The current version is always accessible via the Company's internal compliance portal and published on **domus-x.io** under "Legal & Compliance."

19. Record of Amendments

Version Date	Description of Change	Approved By
1.0	Initial adoption of AML/CTF Policy	Board of Managers
1.1	Annual review – minor updates	AMLCO
1.2	Revised for regulatory guidance	Board of Managers

20. Contacts and Escalation

AML Compliance Officer (AMLCO):
Name: _____
Title: _____
Email: **legal@domus-x.io**
Phone: Available to regulators on request

Mailing Address:
DMSX Token LLC
8 The Green, STE B
Dover, Delaware 19901 USA

Emergency Contact for Law Enforcement:
Available 24/7 via legal@domus-x.io