KYC & AML Policy

Sustainable Digital Assets (SDA)

Version 1.2
Last updated: 14 November 2025

Summary

This policy explains how SDA identifies and verifies customers, applies AML/CTF controls, and implements the Crypto-Asset Transfer Rule. We operate a phased onboarding model: Phase 1 (presale utility-token access) and Phase 2 (regulated security-token/equity features).

Primary contacts:

- **Compliance:** compliance@sdafintech.com
- **DPO:** privacy@sdafintech.com

Key Points

- Below €1,000 cumulative: wallet and IP identification.
- €1,000 or higher: Full KYC is mandatory.
- CDD applies at €1,000–€49,999 (or earlier if risk/law triggers). EDD applies at ≥ €50,000 (single or rolling 12-month cumulative), or earlier for PEPs, high-risk geographies/sectors, sanctions hits, adverse media, complex SoW/ownership, or legal requirements.
- Travel Rule data exchanged on all external crypto transfers; self-hosted wallets > €1,000 require ownership proof.
- Periodic reviews: high-risk or trigger-based only.
- Phase 2 access (security-token/equity features) requires Full KYC/KYB, refreshed screening, investor categorization, and Travel-Rule-ready wallets.
- We do not onboard or service Prohibited Business Activities; see Sanctions & Restricted Territories for full sanctions controls.

---

1. Scope & Legal Basis

This policy covers onboarding, monitoring, and off-boarding of natural persons and legal entities interacting with SDA's token lifecycle. We follow applicable EU AML/CFT rules (including the Crypto-Asset Transfer Rule) alongside investor-protection duties where relevant. Local laws may impose additional requirements in certain jurisdictions.

This policy is complemented by Section 11 (Prohibited Business Activities) and Section 12 (Sanctions & Restricted Territories), which define risk appetite exclusions. Customer acceptance and restrictions follow Sections 11–12.

2. Phase 1 — Presale / Utility-Token Access

Who: presale participants and holders during the utility-token phase.

We collect (everyone):

- Self-declaration: PEP status and sanctions screening.
- **Wallet checks:** proof of ownership (signed message or micro-transaction loopback) for payout/withdrawal addresses.

Tiering during Phase 1:

- **Tier A (under €1,000 cumulative, low risk):** – Wallet and IP identification only. – Self-declaration PEP/sanctions status; geofencing for restricted countries.
- **Tier B (≥ €1,000 or heightened risk):** – Photo ID capture + automated liveness/face-match or robust bank-KYC evidence (e.g., SEPA account in same name). – **Full KYC** before further funding, voting, withdrawals or profit-sharing; apply EDD where flags exist. – **CDD:** applies to €1,000–€49,999 unless risk/law requires earlier EDD. – **EDD:** mandatory at ≥ €50,000 (single or rolling 12-month cumulative), or earlier where risk/law requires.

3. KYC/KYB Requirements (All Phases)

Individuals

- Government ID (passport/ID card/driver's license) + liveness/face-match; second document if needed.
- **Proof of address** (≤3 months): utility bill, bank/credit statement, government letter.
- Sanctions/PEP/adverse media cleared; PEPs require senior approval (EDD).
- Purpose & intended use; expected activity profile.
- **Source of Funds** (SoF) for the transaction; **Source of Wealth** (SoW) where size/risk warrants
- Ongoing monitoring; periodic reviews only for high-risk customers or when risk triggers occur (e.g., PEP status change, sanctions hit, alerts).

Entities (KYB)

- Legal name, registration number, registered address, formation documents/registry extract; LEI where available.
- **Ownership & control:** identify UBOs ≥25% or effective control; verify proxies/representatives (directors/signatories); Full KYC on UBOs and directors/signatories
- Business profile, licenses (if applicable), expected activity.
- SoF/SoW at entity and UBO levels as appropriate.
- Sanctions/PEP/adverse media at entity/UBO/director levels; ongoing monitoring with periodic reviews only for high-risk or trigger-based cases.

4. Phase 2 — Security-Token / Equity Features

Who: clients converting to, receiving, or transacting SDA's regulated security-token and any equity-linked rights.

Required before Phase 2 access:

- Completed **Full KYC/KYB** (ID + proof-of-address + screening).
- Provided **SoF/SoW** aligned to investment size.
- **Refreshed screening:** sanctions/PEP
- Declared **investor category;** completed any required questionnaires.
- Registered **wallets** with ownership proof (especially for self-hosted > €1,000).
- Acknowledged policy & disclosures.

5. Travel Rule (Crypto Transfers)

We collect and transmit required **originator/beneficiary** data for external crypto-asset transfers. For **CASP-to-CASP** transfers, we exchange data using industry-standard messaging. For **self-hosted wallets**, we apply **ownership-proof** procedures; above **€1,000**, we verify control (message-sign or loopback transaction). Transfers lacking minimum data or with unresolved red flags are **rejected or held** pending review.

6. Risk-Based Approach & EDD

We score risk across **customer, geography, product, delivery channel,** and **behavior**. Transaction monitoring: address/IP for < €1,000; enhanced monitoring for ≥ €1,000. **Risk levels:** Low (CDD) and High (EDD). **EDD triggers:** (i) single transaction ≥ **€50,000**; (ii) cumulative funding ≥ **€50,000** in any rolling 12 months; or earlier for PEPs, high-risk jurisdictions/sectors, sanctions hits, adverse media, complex ownership/SoW, unusual velocity/structuring, or other legal requirements. **EDD measures** may include SoW verification, enhanced documentation, senior-management approval, lower limits, or refusal/exit. Customers engaged in Prohibited Activities (Section 11) are not eligible for onboarding or continued servicing. Suspicious activity: investigate internally and, where required, file reports to the competent FIU/law-enforcement.

7. Acceptable Documents (Annex)

ID: passport; national ID; driver's license (where accepted).

Address: bank/credit statement, utility bill, government letter, lease/tenancy (with authority contact), property tax.

SoF/SoW (examples): pay slips, employment contract, audited statements, tax returns, company sale docs, property sale docs, inheritance/probate, exchange withdrawal history with bank trails, etc.

8. Data Protection & Retention

We store only data needed for AML/CTF, onboarding, servicing, and legal obligations. KYC and transactional records are retained for the legally required period and then **deleted or anonymized**. You may exercise privacy rights via **privacy@sdafintech.com** (subject to AML retention exemptions). Staff receive ongoing AML/CTF training.

9. Record-Keeping

We maintain reproducible records of **who was identified, how, and when**, including screening results, SoF/SoW evidence, investor categorization (Phase 2), and Travel Rule data exchanges.

11. Prohibited Business Activities

To comply with applicable AML/CTF, sanctions, and financial-services regulations, SDA prohibits any use of the **SDA Token** or participation in the **SDA Token Sale** by, or on behalf of, persons or entities engaged in the businesses or activities listed below (together, the *"Prohibited Activities"*). SDA may refuse onboarding, block transactions, suspend or exit relationships, and make regulatory filings where required. This list is illustrative, not exhaustive.

11.1 Privacy-Enhancing Technologies

- Development, promotion, or facilitation of privacy coins, mixers, tumblers, or other technologies designed to obfuscate transaction trails or enhance financial anonymity beyond standard cryptocurrency features.

11.2 Gambling and Betting

- Online or offline gambling, betting, gaming, or lottery services (including prediction markets, fantasy sports, and casino operations).

11.3 Adult Content and Pornography

- Production, distribution, or facilitation of pornographic content, escort services, or other adult entertainment.

11.4 Weapons and Military Trade

- Sale, manufacture, or distribution of firearms, ammunition, military equipment, dual-use goods subject to export controls, or other weapons.

11.5 Drugs and Controlled Substances

- Sale, distribution, or facilitation of illegal drugs, controlled substances, or pharmaceutical products without proper authorization.

11.6 Human Exploitation and Trafficking

- Activities involving forced labor, human trafficking, child exploitation, or modern slavery.

11.7 Other Illegal or High-Risk Activities

- Any activity that is unlawful in the jurisdiction where it is carried out, or that in SDA's sole discretion presents unacceptable AML/CTF, sanctions, or reputational risk.

12. Sanctions & Restricted Territories

SDA complies with sanctions regimes administered by the United Nations, United States (OFAC), European Union, and United Kingdom, and applies a risk-based approach to high-risk jurisdictions identified by FATF.

12.1 Scope & Data Sources

- Screening at onboarding and on an ongoing basis against UN/OFAC/EU/UK lists (individuals, entities, vessels).
- Jurisdictional risk based on FATF lists (*High-Risk Jurisdictions subject to a Call for Action*; *Jurisdictions under Increased Monitoring*) and SDA's risk appetite.
- Geolocation controls (IP/device), payment-rail risk flags, and wallet provenance checks.

12.2 Controls

- **Prohibited:** customers located in, organized in, or ordinarily resident in comprehensively sanctioned countries; transactions that would breach sanctions.
- **Restricted:** targeted sanctions (e.g., SDNs/asset freezes) — block, report, and do not onboard/service.
- **High-risk jurisdictions (FATF grey list):** apply enhanced due diligence, lower limits, or decline per risk appetite.
- **Escalation:** Compliance approval for any edge case; licenses/authorizations documented where applicable.

12.3 Enforcement & Record-Keeping

We may refuse onboarding, block or exit relationships, freeze assets/transfers where required, and make required regulatory filings. Screening results and decisions are recorded per **Record-Keeping**.

13. Contact Compliance

Questions or escalations:

Sustainable Digital Assets Inc.
Corporation Number: C 61288
LEI: 89450058XEES8WCSCQ03
Huggins House
P.O. Box 187
Old Manor Estate
Gingerland, Nevis
Compliance: compliance@sdafintech.com

14. Revision History

v1.2 — 14 Nov 2025: Defined CDD/EDD thresholds (€1,000–€49,999 / ≥€50,000); risk-based periodic reviews; enhanced entity verification.

v1.1 — 22 Aug 2025: Added Prohibited Business Activities section; expanded Sanctions & Restricted Territories controls.

v1.0 — 18 Aug 2025: Initial publication; Phase 1/Phase 2 split; Travel Rule procedures; investor categorization for Phase 2.

Frequently Asked Questions

Q: Do I need KYC below €1,000?

A: Yes—below €1,000 we require wallet and IP identification plus self-declaration. Full KYC starts at €1,000 cumulative or if risk flags appear.

Q: When do you apply EDD?

A: At €50,000 (single transaction or rolling 12-month cumulative), or earlier for PEPs, high-risk jurisdictions/sectors, sanctions hits, adverse media, complex ownership/SoW, unusual velocity/structuring, or legal requirements.

Q: What's different in Phase 2?

A: You must complete Full KYC/KYB, refresh screening, provide SoF/SoW, declare investor category, and use Travel-Rule-ready wallets.

Q: Can I use a self-hosted wallet?

A: Yes, with ownership proof; above €1,000 we require signed-message or micro-transfer verification.

Q: How long do you keep my data?

A: For the legally required period to meet AML/CTF obligations; then we delete or anonymize.

Q: I'm a company — what's required? A: KYB docs, UBO identification (≥25% or effective control), Full KYC on UBOs/directors, and SoF/SoW evidence.

Huggins House, P.O. Box 187, Old Manor Estate, Gingerland, Nevis
Tel: +358 30 623 0300 - Email: compliance@sdafintech.com