UNIFIEDX / CONTROLLED PUBLICATION

AML, Sanctions & KYC Policy

Risk-based controls for OTC, partner, legal and higher-risk activity, with public incident-response governance.

EFFECTIVE / LAST UPDATED	**16 August 2026**
SCOPE	**AML/CFT/CPF, sanctions, KYC/KYB and OTC security controls**
PUBLICATION	**unifiedx.io**

This PDF is the publication copy of the corresponding UNIFIEDX website policy. On-chain addresses and transaction hashes are disclosed in full. Users should compare live blockchain state before transacting; source and bytecode matching does not guarantee the absence of vulnerabilities.

SECTION 01

Purpose, Status and Interpretation

This AML, Sanctions & KYC Policy (the "Policy") explains the risk-based controls UNIFIEDX may apply to prevent money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud and other unlawful use of its products and infrastructure.

UNIFIEDX provides non-custodial software and blockchain infrastructure. Unless a service-specific agreement expressly states otherwise, UNIFIEDX does not hold users' private keys, recovery phrases or self-hosted-wallet assets, and does not initiate or sign transactions for users.

Non-custodial architecture does not eliminate compliance obligations. Controls depend on the service used, the parties, transaction risk, applicable law, partner requirements and the regulatory classification of the actual business activity in the relevant jurisdiction.

This Policy is a public description of UNIFIEDX controls. It is not legal advice, a representation that every service is regulated in the same way, or a substitute for service-specific terms, mandatory law or an applicable privacy notice. Where they conflict, mandatory law and transaction-specific requirements prevail.

SECTION 02

Services Covered by This Policy

This Policy may apply to access to or use of the UNIFIEDX website, dashboard, Exchange Terminal, cross-chain routing, limit-order tools, OTC and smart-contract escrow interfaces, On-Chain Intelligence, token-building tools, APIs, partner integrations and future products.

The intensity of controls is proportionate to risk. A standard non-custodial interface may be available without blanket identity verification, while an OTC transaction, a regulated partner route, a higher-risk wallet or a legally defined threshold may require KYC, KYB, enhanced due diligence or refusal of service.

A service being visible in the interface does not guarantee that it is available to every person, wallet, entity, jurisdiction or transaction.

SECTION 03

Key Definitions

- AML/CFT/CPF means controls against money laundering, terrorist financing and proliferation financing;
- KYC means identifying and verifying an individual customer or user;
- KYB means identifying and verifying a legal entity, its activities, ownership and control;
- UBO means the natural person or persons who ultimately own or control an entity, applying the threshold and control tests required by applicable law or a lower risk-based threshold where appropriate;
- PEP means a politically exposed person, including relevant family members and close associates where required;
- KYT means risk analysis of wallets, blockchain transactions and their direct or indirect exposure;

- EDD means enhanced due diligence applied where elevated risk requires additional information, evidence, approval or monitoring;
- Source of Funds means the origin of assets used in a particular transaction, while Source of Wealth means how a person's overall wealth was accumulated.

SECTION 04

Risk-Based Approach

UNIFIEDX assesses risk using the information reasonably available at the relevant time. A risk assessment may consider the customer, beneficial owners, counterparties, product, transaction size and pattern, wallet history, asset, blockchain, geography, delivery channel, sanctions exposure, partner requirements and the quality or consistency of information supplied.

Controls may include automated rules, blockchain analytics, sanctions and PEP screening, adverse-media review, manual review, additional documentation, transaction limits, senior approval, ongoing monitoring and periodic re-screening.

A risk signal is not necessarily proof of unlawful conduct. Where appropriate and legally permitted, material alerts are reviewed in context before a final service decision is made.

SECTION 05

When KYC May Be Required

UNIFIEDX does not promise universal or continuous KYC for every ordinary non-custodial interaction. Identity verification may nevertheless be required before, during or after a service request when one or more of the following applies:

- the user starts, negotiates, funds, fills or otherwise participates in an OTC or escrow-supported transaction;
- applicable law, a competent authority, court order, licence condition or regulatory threshold requires verification;
- a bank, liquidity source, exchange, bridge, on-ramp, off-ramp, compliance provider or other service partner requires verification;
- a transaction, wallet, counterparty, asset, location, device or behaviour presents elevated risk;
- screening indicates a potential sanctions, PEP, adverse-media, fraud, stolen-funds or other compliance match;
- information is missing, inconsistent, expired, difficult to verify or reasonably suspected to be false;
- ongoing due diligence, a material change in activity or a review of an existing relationship requires updated information.

If required verification is not completed to UNIFIEDX's reasonable satisfaction, the affected service may not be provided even if the user's wallet remains independently accessible on-chain.

SECTION 06

Individual KYC Information

Depending on risk and applicable law, UNIFIEDX or an approved verification provider may request only the data reasonably necessary for the review, which may include:

- full legal name, date and place of birth, nationality and country of residence;
- residential address, email address and telephone number;
- a valid government-issued identity document and its relevant details;
- a selfie, video or liveness check to confirm that the applicant is the document holder;
- proof of address, tax or national identification number where legally required;
- occupation, employer or business activity, expected use and anticipated transaction profile;
- evidence of wallet ownership or control, transaction purpose and counterparty relationship;
- source-of-funds or source-of-wealth information where risk requires it.

Documents must be authentic, current, legible and belong to the person being verified. UNIFIEDX may require certified, notarised or translated copies where reasonable and proportionate.

SECTION 07

KYB and Beneficial Ownership

Legal entities may be required to complete KYB before accessing an eligible service. The review may cover:

- legal and trading names, registration number, formation date, registered office and principal place of business;
- constitutional documents, registry extracts, good-standing evidence and relevant licences or permissions;
- business model, products, markets, expected use of UNIFIEDX and anticipated transaction volumes;
- ownership and control structure, including parent entities, subsidiaries, trusts, nominees or other arrangements;
- directors, senior managers, authorised representatives and persons able to instruct or control transactions;
- each UBO and any other natural person exercising ultimate control;
- financial information, source of funds, source of wealth and supporting commercial documents when required.

UNIFIEDX may look through intermediate companies and legal arrangements until the relevant natural persons are identified. If ownership or control cannot be established, the service may be refused.

SECTION 08

Sanctions, PEP and Adverse-Media Screening

UNIFIEDX may screen users, entities, UBOs, directors, representatives, counterparties, wallet addresses and relevant connected persons against applicable sanctions and restrictive-measures lists, including lists maintained by the United Nations, the United States, the European Union, the United Kingdom and competent local authorities.

Screening may also identify PEP status, family members and close associates, public-office connections, state-owned-enterprise exposure, disqualification records, law-enforcement information and credible adverse media relating to financial crime, corruption, fraud or other serious misconduct.

A possible name match may require further identifying information. Confirmed sanctions exposure or an unacceptable sanctions-evasion risk may result in refusal, restriction, reporting or other action required by law.

SECTION 09

AML/KYT Wallet and Transaction Analysis

UNIFIEDX may analyse blockchain addresses, transaction hashes, counterparties, asset flows and direct or indirect exposure using internal methods and third-party blockchain-analytics tools.

Relevant indicators may include exposure associated with sanctions, terrorist financing, ransomware, theft, scams, fraud, hacks, darknet markets, child exploitation, illicit gambling, corruption, high-risk services, obfuscation services, peel chains, rapid chain-hopping, unusual transaction patterns or other typologies identified by competent authorities.

Wallet-risk scores and attribution labels may contain uncertainty. UNIFIEDX may request an explanation, evidence of ownership, transaction records or counterparty information to resolve an alert.

SECTION 10

OTC and Smart-Contract Escrow Controls

OTC activity generally presents higher counterparty, fraud, sanctions and source-of-funds risk than an ordinary self-directed interface. UNIFIEDX may therefore require KYC or KYB for the maker, taker, beneficial owners and authorised representatives before providing or continuing an OTC-related service.

Before an OTC deal is accepted or supported, UNIFIEDX may review the parties, deal purpose, asset pair, wallet ownership, transaction history, pricing, size, geographic nexus, counterparty relationship, supporting agreement and source of funds. EDD or compliance approval may be required for material or higher-risk transactions.

The active non-custodial OTC contract holds assets according to immutable settlement logic without an administrator withdrawal or upgrade function. Compliance action by UNIFIEDX normally concerns accepting or supporting a deal, requesting information, applying limits or restricting the interface. On-chain rights and exits remain governed by the deployed contract and applicable law.

SECTION 10A

OTC Security Pause, Governance and Public Addresses

UNIFIEDX separates compliance decisions from the contract's emergency incident-response function. A wallet-specific sanctions, KYC, KYB or source-of-funds alert ordinarily leads to review, refusal or interface restriction. It does not by itself enable UNIFIEDX to seize or freeze assets in a self-hosted wallet.

A global emergency pause is reserved for a reasonably credible and immediate system-level threat—for example, an active or imminent exploit, attempted hack, suspected compromise of a governance signer, material bytecode or role mismatch, malicious on-chain behaviour indicating contract abuse, or a BNB Smart Chain or critical dependency incident capable of causing unauthorized transfers or unsafe settlement.

Starting the pause requires a Safe transaction approved by both disclosed owners. It blocks new order creation and fills for a maximum of 48 hours. It does not block maker cancellation, expiry reclamation or withdrawal of credited native assets; it cannot reverse a completed transfer, redirect escrowed assets or freeze an external wallet. The owner-only unpause function is behind the same 48-hour timelock and therefore ordinarily cannot shorten a newly started pause. After the deadline, any blockchain account may clear the stale pause.

Network	BNB Smart Chain mainnet — chain ID 56
OTC escrow	0x0bb6E592C81570D5070BA327F5B8237D5F72b282
48-hour governance timelock / escrow owner	0x0c8dB0ac2Da3FdfEb2B2DDFC36867Cc3f680aA3E
Safe emergency guardian	0x9e3A2BAA6dfcC2327246aB031f2Aa6788E6f7773
Safe owner 1	0x65A0c9678435aCbB3948e8eD0f1085b3Ad074712
Safe owner 2	0x1Bf301dA72d562adc9030af76fAC2A3CA8720b53
Approval threshold	2 of 2 owner signatures
Safe version / singleton	1.4.1 — 0x29fcB43b46531BcA003ddC8FCB67FFE91900C762
Safe proxy factory	0x4e1DCf7AD4e460CfD30791CCC4F9c8a4f820ec67
Safe fallback handler	0xfd0732Dc9E303f09fCEf3a7388Ad10A83459Ec99
Optional Safe Guard	Not installed — 0x0000000000000000000000000000000000000000
Safe modules	None enabled

The escrow guardian role and an optional Safe Guard are different controls. The escrow guardian is the Safe 2-of-2 account listed above. The Safe's own optional Guard slot is zero and no module is enabled, so neither can bypass the native 2-of-2 signature rule in the verified configuration.

The deployment was verified through BscScan creation transactions and live state, Sourcify exact source-to-creation/runtime bytecode matching, and a deterministic release verifier that checks runtime hashes, escrow owner and guardian, pending ownership, Safe owners and threshold, singleton, factory, fallback handler, modules, Guard slot, timelock roles and the 48-hour parameters.

Safe creation transaction	0x5763d57034f13a19641dfed643238217b47155dab040d1a6b28c854847b38be6
Timelock creation transaction	0x1a26bd0784526fcac6897f1f3fc030f2d8c91b7974f5f00763fdf054b9f0f259

Escrow creation transaction	0x6643f196ab0b3a8a385cf814753d0cd9db50d1db795e96cb6f7937714739cc6d
Timelock runtime hash	0x9d2696dab825e8732c9d1cd112a97194300b80f420fc9bfdf5e67f5053c4cf61
Escrow runtime hash	0xc1bbfbe87930ff29025b7f3d9b4c6cc67fecc3c4de445db1a0c0876661100a6a
Sourcify timelock exact match	Match ID 43700363
Sourcify escrow exact match	Match ID 43700365
Source verification timestamp	16 August 2026, 19:11:44 UTC

If a pause is activated, the incident process should record the detected indicator and evidence, distinguish a cyberattack from a compliance alert, confirm both Safe approvals on-chain, preserve relevant logs and transaction data, communicate service impact where legally permitted, and reassess whether safe operation can resume. Verification records demonstrate configuration and source matching, but do not guarantee the absence of vulnerabilities or replace transaction-specific compliance review.

SECTION 11

Source of Funds and Source of Wealth

For higher-risk or material OTC transactions, UNIFIEDX may request evidence showing how the specific assets were obtained and, where appropriate, how the user's broader wealth was accumulated.

- wallet histories, transaction hashes and evidence linking a wallet to the applicant;
- regulated-exchange or custodian statements;
- bank statements or payment records;
- sale, investment, loan or inheritance documents;
- invoices, audited accounts, payroll, dividend, tax or mining records;
- token-allocation, vesting, staking or protocol-reward evidence;
- other reliable documents explaining the economic purpose and origin of funds.

The type and depth of evidence requested will depend on risk. UNIFIEDX may verify authenticity, seek clarification and decline unsupported, implausible or inconsistent explanations.

SECTION 12

Enhanced Due Diligence

EDD may be applied to PEPs, complex or opaque ownership, higher-risk jurisdictions, unusually large or complex transactions, privacy-enhancing or obfuscation exposure, high-risk business activity, unexplained third-party funding, negative information or other elevated-risk circumstances.

EDD may include additional identity or corporate evidence, independent database checks, a video interview, source-of-funds and source-of-wealth verification, transaction-purpose evidence, senior compliance approval, lower limits, enhanced monitoring, restricted products or periodic refresh.

SECTION 13

Restricted and Prohibited Jurisdictions

A person may not use an affected UNIFIEDX service from, for the benefit of, or on behalf of a jurisdiction or territory where the service is unlawful, requires an authorisation that is not held, is subject to applicable comprehensive territorial sanctions, or is prohibited by an applicable partner or provider.

UNIFIEDX may also restrict services involving jurisdictions identified by FATF for a call for action, jurisdictions with material AML/CFT deficiencies, or locations that cannot be reliably verified, where a proportionate risk assessment supports restriction.

Official lists and legal restrictions change. Eligibility is determined against the rules in force at the time of access or review. Users must not use a VPN, proxy, nominee, shell entity, false address or other method to conceal location or circumvent a geographic restriction.

SECTION 14

Prohibited Activities

UNIFIEDX services must not be used directly or indirectly for:

- money laundering, terrorist or proliferation financing, sanctions evasion or activity involving blocked persons or property;
- fraud, scams, theft, extortion, ransomware, malware, hacking, phishing or trafficking in stolen assets or credentials;
- darknet commerce, child sexual exploitation, human trafficking, illegal narcotics, corruption, bribery or other serious crime;
- deceptive market activity, wash trading, manipulation, misappropriation or circumvention of legal transaction controls;
- illegal gambling, unlicensed financial or money-service activity, shell banks or businesses operating without required permissions;
- weapons, counterfeit goods or other restricted trade where unlawful;
- obscuring beneficial ownership, submitting false information, impersonation, nominee misuse or structuring activity to avoid review thresholds;
- any other activity that violates applicable law, the UNIFIEDX Terms & Conditions or a service-specific restriction.

SECTION 15

Refusal, Restriction and Other Service Decisions

Where permitted or required, UNIFIEDX may request more information, delay a service review, decline to quote or facilitate a transaction, reject an OTC request, apply limits, disable a feature, restrict access to an interface, suspend or terminate provision of a service, end a partner route, preserve relevant records or make a legally required report.

UNIFIEDX may be unable to explain a decision in full where disclosure is restricted by law, could prejudice an investigation, reveal confidential risk controls or create unlawful tipping-off.

Because UNIFIEDX is non-custodial, it does not claim that it can freeze assets held in a user's self-hosted wallet or reverse a confirmed blockchain transaction. Restricting the UNIFIEDX interface or service does not prevent a user from accessing an independent blockchain through other means.

SECTION 16

Ongoing Monitoring and Review

Compliance is not necessarily completed once at onboarding. UNIFIEDX may monitor supported activity, re-screen parties and wallets, refresh documents, review material changes, update risk ratings and investigate alerts for as long as a relevant service relationship or legal obligation continues.

Users must promptly provide accurate updates if identity, address, ownership, control, authorisation, business activity, transaction purpose or source of funds materially changes.

SECTION 17

Transfers, Partners and the Travel Rule

Where UNIFIEDX or an integrated provider is legally treated as an obliged entity or crypto-asset service provider for a relevant transfer, originator and beneficiary information may have to be obtained, verified, retained or transmitted under applicable transfer-of-funds or Travel Rule requirements.

Requirements differ by jurisdiction, provider and transaction. A self-hosted-wallet transfer may require proof of wallet ownership or control and counterparty information where applicable. UNIFIEDX may decline a route if required information cannot be lawfully or securely exchanged.

SECTION 18

Suspicious Activity and Authorities

Where legally required, UNIFIEDX or the relevant regulated provider may submit suspicious-activity, sanctions or other reports; respond to lawful requests; preserve records; and cooperate with competent regulators, financial-intelligence units, courts or law-enforcement authorities.

Nothing in this Policy requires UNIFIEDX to notify a user of a confidential report, investigation or legally restricted request.

SECTION 19

Recordkeeping

UNIFIEDX and its providers may retain identity, verification, risk, communications and transaction-related records for the period required by applicable law and legitimate compliance needs. Where a five-year AML retention period applies, records may generally be kept for at least five years after the relevant relationship or transaction, subject to local rules.

Records may be retained longer where required by a legal hold, investigation, dispute, sanctions obligation or limitation period, and deleted or anonymised when retention is no longer lawfully justified.

SECTION 20

Personal Data and Security

KYC and AML reviews may involve sensitive identity, biometric, corporate, financial, device and blockchain data. UNIFIEDX seeks to limit collection to what is necessary and to protect information using proportionate organisational and technical safeguards, access controls and vendor oversight. No system can guarantee absolute security.

This Policy is not a privacy notice. Before UNIFIEDX directly collects identity documents or comparable KYC data, the user will be provided with the applicable privacy information describing the controller, purposes, legal bases, sharing, transfers, retention, rights and contact route required by law.

Users should not send identity documents by ordinary email unless specifically instructed through an approved secure process.

SECTION 21

Third-Party KYC and AML Providers

UNIFIEDX may use specialist providers for document and biometric verification, company-registry checks, sanctions and PEP screening, adverse-media research, fraud prevention, wallet analytics, Travel Rule messaging, secure storage and case management.

Providers process data under their own or UNIFIEDX's legal responsibilities as applicable. Information may be processed in other countries subject to required safeguards. UNIFIEDX may change providers and may withhold certain vendor or control details where disclosure would create a security or circumvention risk.

A provider result supports but does not necessarily determine UNIFIEDX's final risk decision.

SECTION 22

User Representations and Cooperation

By requesting an affected service, the user confirms that information and documents supplied are accurate, complete, current and lawfully provided; that the user acts for themselves or has disclosed and is authorised to act for the relevant principal; and that the service will not be used for prohibited activity.

The user must answer reasonable compliance requests within the stated time, must not tamper with documents or screening, and must not split or route transactions to evade controls. Failure to cooperate may result in refusal or restriction.

SECTION 23

Review of a Compliance Decision

A user may request review of a service restriction by contacting UNIFIEDX with the relevant case or transaction reference and a concise explanation. UNIFIEDX may request additional evidence and will review the request where legally permitted.

A review request does not guarantee reversal, does not delay a legal obligation and may not be available for decisions controlled by an independent provider or competent authority.

SECTION 24

Regulatory Classification and No Waiver

The regulatory treatment of software, virtual-asset services, OTC support, smart-contract interfaces and related activities depends on facts and jurisdiction. This Policy does not itself classify UNIFIEDX as a VASP, CASP, financial institution, money transmitter, exchange, broker, custodian or other regulated person in every jurisdiction.

Applying a voluntary or partner-required control does not concede that a specific legal obligation applies. Conversely, an omission from this public Policy does not prevent UNIFIEDX from applying a control required by law or reasonably necessary to manage risk.

SECTION 25

Policy Changes

UNIFIEDX may update this Policy to reflect changes in products, risk, law, guidance, partners or compliance operations. The current version will be published at unifiedx.io/aml-kyc with its effective date.

Material changes may be communicated through the interface or another reasonable channel where required. Continued use after an effective date is subject to the updated Policy and applicable law.

SECTION 26

Compliance Contact

For compliance questions or a permitted review request, contact UNIFIEDX Compliance through the address below and use the subject line "Compliance Review". Do not attach identity documents unless you are directed to an approved secure upload flow.

SECTION 27

Regulatory References

This Policy is informed by the following official materials. A reference does not mean that every instrument directly applies to every UNIFIEDX product or user.

FATF — Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs	https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf
FATF — Virtual Assets Hub	https://www.fatf-gafi.org/en/topics/virtual-assets.html
OFAC FAQ 560 — Digital Currency and Risk-Based Sanctions Compliance	https://ofac.treasury.gov/faqs/560
EU Regulation 2023/1113 — Information Accompanying Transfers of Funds and Certain Crypto-assets	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1113

Policy Summary

- ordinary non-custodial use does not automatically mean blanket KYC;
- OTC, partner, legal and higher-risk activity may require KYC, KYB or EDD;
- wallet and transaction screening may be used to assess financial-crime risk;
- UNIFIEDX may decline a transaction or restrict its interface without claiming custody of a user's wallet assets;
- users must provide accurate information and may not circumvent controls.