CYPHERVEST INSTITUTIONAL USER COMPLIANCE & POLICY TERMS

OFFICIAL SYSTEM-OPERATOR REGISTRY | GOVERNANCE FRAMEWORK v2.0

Document Registry Metric	Registry Entry Value
DOCUMENT REF	CV-TERMS-2026-INSTITUTIONAL-V2.0
EFFECTIVE DATE	01 Jan, 2026
PROTOCOL	Tezos LPoS (Liquid Proof-of-Stake)
COMPLIANCE	UK eIDAS & ESIGN Compliant

ARTICLE I: PREAMBLE & SYSTEMIC MANDATE

Section 1.1: System-Operator Status Cyphervest (hereinafter "The Operator") functions as the primary cryptographic System-Operator for tokenized Real-World Assets (RWAs). This framework governs all interaction, digital property registration, and cryptographic execution within the Tezos Liquid Proof-of-Stake (LPoS) decentralized network.

Section 1.2: System Boundaries This document establishes the legally binding boundaries and technical parameters of institutional user interaction within the ecosystem. The systemic mandate prioritizes long-term Environmental, Social, and Governance (ESG) aligned sustainability.
Every synergistic commitment, asset-backed transaction, and settlement cycle executed on-chain is backed by immutable cryptographic proof and verified physical or financial value. Participation in the platform constitutes an explicit, irrevocable agreement to adhere to these governance protocols without reservation.

ARTICLE II: IDENTITY AUTHENTICATION & ONBOARDING

Section 2.1: High-Assurance Onboarding Pipeline To safeguard the system from compliance failures, institutional onboarding is subject to an exhaustive twenty-one (21) working day Know Your Customer (KYC) and Anti-Money Laundering (AML) validation window. During this authentication period, all assets and deposits remain locked in a non-transferable, non-yield-bearing "Pending Registry" state.

The Operator reserves the absolute right to deny platform activation or confiscate registry access from any entity failing to meet the rigorous identity verification standards set by UK eIDAS, the US ESIGN Act, and global financial safety protocols.

Section 2.2: UK eIDAS & Digital Seal Integration Legal entities interacting with the platform must authenticate their corporate identity utilizing Qualified Electronic Seals (QSeals) issued by an accredited Qualified Trust Service Provider (QTSP) under UK eIDAS or EU Regulation No 910/2014 (as adopted into UK law).

CYPHERVEST INSTITUTIONAL USER COMPLIANCE & POLICY TERMS

All organizational authorizations, compliance representations, and transaction signatures must satisfy the requirements of Advanced or Qualified Electronic Seals :

Seal/Signature Class	Cryptographic Binding Requirement	Legal Presumption of Authenticity
Advanced Electronic Seal (AdES)	Unique linkage to the entity; detects subsequent modification.	Admissible in court with evidence of cryptographic integrity.
Qualified Electronic Seal (QES/QSeal)	Created via a Qualified Signature/Seal Creation Device (QSCD).	Equivalent to a handwritten signature and physical stamp across jurisdictions.

ARTICLE III: DIGITAL PROPERTY RIGHTS & TOKENIZATION

Section 3.1: MLETR Enforceability and Exclusive Control All cryptographic stakes and digital assets recorded on the Tezos Ledger are legally classified as enforceable digital property interests. These interests are mathematically mapped 1:1 to verified physical or financial assets held in secure, bankruptcy-remote custody.

The technical architecture is specifically structured to comply with the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Transferable Records (MLETR). To satisfy the MLETR framework, the underlying protocol enforces functional equivalence through two core parameters:

1. **The Singularity Requirement:** Employs unique on-chain token identifiers to prevent duplicate claims on a single underlying obligation.
2. **The Control Requirement:** Employs public-key cryptography to establish "exclusive control". A transaction is legally validated when signed by the private key of the recognized holder.

Section 3.2: Multi-Asset FA2 Token Standards The tokenization ledger is executed using the Tezos FA2 (TZIP-12) or FA2.1 multi-asset token standards. Each distinct asset class is assigned a unique token_id. The contract utilizes strict type-safety boundaries :

FA2 Entrypoint	Technical Parameter Definition	Regulatory/Legal Compliance Role
transfer	(address %from, list %requests)	Executes the transfer of exclusive control and possession of the digital record.
balance_of	(list %requests, contract %callback)	Provides a real-time, auditable record of token ownership directly from contract storage.
update_operators	(list %commands)	Regulates delegation of transfer rights to approved

CYPHERVEST INSTITUTIONAL USER COMPLIANCE & POLICY TERMS

FA2 Entrypoint	Technical Parameter Definition	Regulatory/Legal Compliance Role
		compliance or escrow smart contracts.

To protect the system against precision-drift exploits and inflation-based dilution attacks, all arithmetic operations enforce strict rounding rules that favor the contract. The system rounds down when calculating token distributions or deductions, and rounds up when applying policy-driven fees or compliance criteria.

ARTICLE IV: LIQUIDITY GOVERNANCE & MERITOCRACY

Section 4.1: Unstake-Meritocracy Protocol Withdrawals, redemptions, and asset liquidations are governed exclusively by the "Unstake-Meritocracy Protocol". This protocol prevents systemic bank-runs and maintains pool equilibrium by prioritising withdrawals based on participant tier and the duration of their commitments.

Section 4.2: Enshrined Liquid Staking (sTEZ) The core liquidity engine utilizes Enshrined Liquid Staking (sTEZ) built directly into the Tezos protocol layer, eliminating the administrative key risks associated with third-party staking intermediaries. The token uses an accrual model. The exchange rate (R_t) at block level t is defined as :
R_t = \frac{L_t}{S_t}

Where:

- R_t is the exchange rate (mutez per sTEZ token).
- L_t is the total amount of tez in the sTEZ staking ledger.
- S_t is the total outstanding supply of sTEZ tokens.

Staking rewards automatically increase L_t while S_t remains constant, raising the exchange rate (R_t). Conversely, slashing events decrease L_t, reducing the exchange rate (R_t) to distribute losses proportionally across all pool participants.

Section 4.3: Uniform Price Auction & Global Fee Model The protocol allocates staked assets across delegates using a uniform price auction. Participating delegates bid their competitive fees, and the protocol automatically selects the lowest-fee candidates based on validation capacity. The system then applies a "global fee" to all selected delegates, defined as the highest fee among the chosen group :

ARTICLE V: CRYPTOGRAPHIC INTEGRITY & SMART CONTRACTS

Section 5.1: Michelson Architecture and Typestate Security Operational security is anchored in formally verified smart contracts deployed on the Tezos Mainnet. These contracts are written in or compiled down to Michelson, a stack-based, strongly-typed virtual machine

language designed to eliminate typical attack vectors. Michelson prevents reentrancy, overflow, and compiler discrepancies by omitting jump instructions, banning floating-point calculations, and enforcing explicit typed failure states.

Section 5.2: Dual Formal Verification Verification Pathways The integrity of the platform is maintained through continuous formal verification using two complementary environments :

- **Low-Level Code Certification (Mi-Cho-Coq):** Uses the Coq proof-assistant to mathematically model Michelson bytecode, generating formal proofs that confirm the contract logic matches its functional specification.
- **High-Level Architectural Verification (Archetype & Why3):** Utilizes the Archetype domain-specific language to define contract specifications, state-machine transitions, and invariants. Archetype transcodes contract logic into WhyML, generating proof obligations verified via the Why3 verification platform using automated SMT solvers (Alt-Ergo, Z3, CVC4).

ARTICLE VI: REGULATORY REPORTING & DATA PRIVACY

Section 6.1: Zero-Knowledge Shielded Pools (Sapling) To reconcile the tension between institutional privacy and regulatory disclosure requirements, the platform utilizes the Tezos Sapling protocol within its transaction logic. Sapling uses zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) over the BLS12-381 and Jubjub elliptic curves to enable shielded transaction execution.

While entering (shielding) and exiting (unshielding) the pool remains visible on the public ledger, transactions executed within the shielded pool are encrypted. The sender, receiver, and transaction amounts are kept completely private from public view.

Section 6.2: Viewing Key Auditor Access Compliance with international anti-money laundering (AML) and counter-terrorist financing (CTF) standards is maintained through a decoupled key hierarchy :

- **The Spending Key:** Remains offline and is used exclusively by the asset holder to sign transaction commitments and generate zero-knowledge proofs.
- **The Viewing Key:** Can be voluntarily shared with jurisdictional authorities, compliance officers, and auditors. The viewing key decrypts and displays transaction details (including sender, receiver, and amounts) for auditing purposes. It does not grant spending authorization or modify the account state.

ARTICLE VII: LIMITATION OF LIABILITY & RISK ACKNOWLEDGMENT

Section 7.1: Technical Infrastructure Boundaries The Operator provides technical infrastructure, cryptographic compilation tools, and system coordination only. Engagement with cryptographic assets involves inherent financial and market risks.
By signing this attestation, the participant acknowledges that they have performed independent legal and financial due diligence. The Operator shall not be held liable for losses resulting from third-party oracle failures (such as data feed manipulation), global network partitions, or

protocol-level exploits beyond its immediate cryptographic control.

CRYPTOGRAPHIC ATTESTATION RECORD

```
SHA-256 HASH
dbc448d5c955fb61fe386082eb75d2a848bdeadd63d9e741fb7546781d8ffeal
TIMESTAMP               01 Jan, 2026
AUTHORITY               Cyphervest Operations Board
VERIFICATION            On-Chain Registry / Tezos Explorer
```