# Client policies and legal terms

AYOV CAPITAL MANAGEMENT LTD.

Vanuatu proposed services | Version 1.0 | 16 October 2026

This policy book explains the proposed private professional-client service model, onboarding requirements, treatment of information, transaction conditions, complaints and principal risks. It covers fiat asset management and controlled real-asset tokenisation, OTC execution, custody arrangements and conversion. Initial admission is limited to approximately 10–20 approved professional clients.

AYOV CAPITAL MANAGEMENT LTD. is the owner-confirmed name of the proposed Vanuatu applicant. Licensing applications are being prepared; this book does not represent that incorporation, a licence grant or a permission for a particular service has been completed. An existing website, entity or deployed smart contract is not automatically part of the proposed applicant. The provider responsible for an accepted service, its permissions and terms must be identified in the service agreement before business begins.

Client and asset enquiries: assets@ayovcapital.com. Compliance, privacy, complaints and suspected fraud: compliance@ayovcapital.com. Never send a password, private key or recovery phrase to either address.

## 1 User terms and conditions

### Scope and agreement

Website access provides information and enquiry facilities. Browsing, accepting cookies, connecting a wallet or submitting an enquiry does not open an account, accept a trade, approve a client or establish an asset-management mandate. A service begins only after eligibility, necessary permissions and checks are satisfied and the identified provider accepts the relevant written agreement or instruction.

The service agreement must identify provider, client, service, governing law, dispute arrangements, approved countries and any custody or conversion partner. Product-specific signed terms prevail for the particular transaction, subject to mandatory law. These public terms do not remove rights that cannot lawfully be excluded or substitute an unknown entity as contracting party.

### Eligibility and authority

Clients must provide accurate identity, beneficial ownership, professional-client status, authority, tax residence, source-of-funds/wealth and asset information as requested. Clients must promptly notify changes. An agent must evidence authority from the principal. AYOV may decline or restrict a service where required checks cannot be completed, the service is unavailable or the instruction is unlawful.

Clients must protect their credentials, verify official communications and use only approved accounts and wallets. A whitelisted wallet is eligible for the configured route; whitelisting does not guarantee a transaction, confer investment advice or prove asset backing. No person may impersonate another party, bypass controls, use stolen or restricted assets, manipulate markets, exploit systems or submit misleading evidence.

A request for quote is not execution. An accepted quote must state product and contract, chain, amount and unit, price/spread, fees, expiry, funding asset, destination, timing and settlement conditions. Quotes expire as stated. Market information, appraisals and oracle prices are references, not guaranteed realisable prices. Do not send funds or tokens solely on the basis of a website figure or unsolicited message.

Only authorised instructions through agreed channels will be accepted. Changes to beneficiary profiles may require independent verification. Once a valid blockchain transaction is broadcast it may not be recoverable; pending or failed transactions require individual review. AYOV will not label delivery complete without the appropriate confirmation evidence. Cash settlement and blockchain settlement must be reconciled separately.

### Asset management custody and conversion

A fiat asset-management mandate must specify whether the service is discretionary, advisory, administration or execution-only, and define objectives, instruments, limits, liquidity, fees, valuation, reporting and termination. A token holding does not create a discretionary management mandate. Professional-client status does not waive applicable conduct duties.

Custody terms must identify who holds assets or keys, the legal entitlement, segregation, subcustody, release controls, fees and insolvency risks. Clients must not assume that every asset is insured or every token is directly redeemable from the physical custodian. Conversion to or from fiat is subject to the named provider's accepted route, checks, rate, fees and cleared-funds evidence. There is no promise that an API message converts a ledger entry into bank cash.

### Suspension termination and liability

AYOV may pause an affected service for security, sanctions, legal duties, incomplete due diligence or material operational failure, subject to law and the agreement. Restrictions must be proportionate; notification may be limited where prohibited. Closure does not extinguish lawful client rights, unsettled obligations, complaints or required record retention. Withdrawal or redemption proceeds through the accepted product route.

No term excludes liability where exclusion is unlawful, including liability that cannot be excluded for fraud or mandatory client protections. Specific liability allocation, notices, governing law and dispute resolution must be agreed in the service contract. A client may complain without losing access to lawful remedies. Changes to public policies will carry a revision date; material contractual changes require the notice or consent specified in the agreement.

## 2 User admission and AML CFT policy

AYOV's proposed services are private and invitation-only for approved professional clients. Admission requires an assessment of identity, ownership/control, authority, countries, expected activity, funding and asset provenance. AYOV may request certified or independently verifiable records, ownership charts, mandate evidence and information about counterparties. Documents must be supplied through the agreed secure channel, not a public blockchain or an unverified message thread.

Higher-risk relationships, politically exposed persons, complex structures and unexplained transactions require enhanced review. An invitation, existing business relationship, allocation letter or wallet balance does not replace checks. An application may be refused where mandatory information is missing or unacceptable. No public material guarantees approval.

Activity may be monitored against the declared purpose and profile. Wallets and relevant parties may be screened, and additional originator/beneficiary information may be required for virtual-asset transfers. AYOV may lawfully share information with competent authorities and regulated providers. Restrictions on disclosure may prevent explanations of a particular review or report. AYOV does not require clients to disclose private keys or seed phrases.

AML, sanctions and fraud controls are separate from investment suitability and reserve verification. Passing one check does not certify the others. Compliance questions should be directed to compliance@ayovcapital.com. Clients should not send transactions to “test” or bypass eligibility restrictions without accepted instructions.

# 3 Privacy policy

## Responsible provider and information collected

The entity collecting information must identify itself at the relevant collection point or in the service agreement. The proposed Vanuatu applicant must not be presented as controller of legacy records merely by publishing this book. For website, account or legacy-service information, use the operator identified for that service and contact compliance@ayovcapital.com to route a privacy request.

Information may include contact details, identity and verification documents, beneficial ownership, authority, residence, bank profiles, asset provenance, wallet addresses, transaction records, correspondence, security logs and cookie choices. AYOV should collect only information reasonably necessary for the stated purpose. Avoid sending health, unrelated financial or third-party personal information unless specifically required through a lawful secure process.

## Purposes grounds and recipients

Information is used to respond to enquiries, assess admission, verify authority, prevent financial crime and fraud, administer mandates and transactions, reconcile assets, handle complaints, protect systems and meet legal duties. The responsible entity must identify the applicable legal ground for each use. Contract steps, legal obligations and legitimate operational purposes must not be replaced by blanket marketing consent. Optional tracking requires an appropriate separate choice where required.

Information may be disclosed to authorised staff, contracted verification/security/hosting/custody/conversion providers, professional advisers and authorities where lawful and necessary. Access must be limited by purpose and confidentiality. AYOV's policy is not to sell client personal information. A provider list and relevant processing locations must be available for the service; no unspecified jurisdiction is represented as providing equivalent protection.

## International processing and blockchain

Before cross-border processing, the responsible entity must assess applicable transfer requirements and put required contractual or other safeguards in place. A Vanuatu application does not displace privacy laws that otherwise apply. Clients may request information about relevant recipients, processing countries and safeguards, subject to lawful confidentiality restrictions.

Public blockchains expose transaction addresses, amounts and other recorded data to observers worldwide, and entries may be permanent. AYOV must not publish identity documents, bank details or raw due-diligence

evidence on-chain. A wallet can still become identifiable when linked to other information. Blockchain records cannot ordinarily be erased by AYOV. Wallet software, explorers, RPC services and linked third-party sites have their own policies.

### Retention rights and requests

Records are retained for their documented purpose and applicable legal periods, including AML and dispute requirements, then securely deleted or anonymised where appropriate. A valid retention duty or hold may limit deletion. Contact compliance@ayovcapital.com for access, correction, deletion, restriction, portability or objections where applicable. AYOV must verify requests proportionately, explain any lawful refusal and respond within the applicable deadline. Withdrawal of optional consent affects future consent-based processing, not earlier lawful processing. Clients retain complaint rights to the competent authority where applicable.

## 4 Data protection and records policy

AYOV requires clear ownership and classification of public, internal and restricted data. Identity, bank, AML, security and key-related records are restricted. Personnel must receive only the access needed for their role. Shared passwords, public evidence folders and secrets embedded in documents or source code are prohibited. Security measures must be appropriate to risk, with tested access control, secure transmission, backups and recovery.

Records must allow an authorised reviewer to reconstruct onboarding, instructions, approvals, asset admissions, minting, trades, transfers, redemption, payments and administrative changes. Corrections must preserve the original event and an explanation. An evidence hash is a reference to a record, not a replacement for retaining the underlying document and authority.

The retention register must identify record type, legal basis, start event, minimum period, holds and deletion method. AML transaction records and relationship records have different retention start events; they must not be deleted from a blanket website-retention rule. Operational logs and unsuccessful enquiries should not be kept indefinitely without a purpose. Backup deletion must follow a controlled cycle, and recovered data remains subject to applicable deletion restrictions.

Suspected loss, unauthorised disclosure or alteration must be reported internally immediately. The incident lead must contain harm, preserve evidence and assess notification obligations. AYOV must not claim a security certification, audit result or recovery performance without evidence. Material incidents must be communicated to affected parties and authorities where required, with accurate facts and protective steps.

## 5 Sanctions and prohibited activity policy

AYOV prohibits unlawful sanctions evasion, money laundering, terrorism financing, proliferation financing, fraud, market abuse and use of stolen assets. Checks cover customers and relevant owners/controllers, counterparties, providers, banks and wallets. Applicable UN and Vanuatu measures and other regimes with a relevant nexus or contractual requirement must be assessed.

A possible match may delay an instruction while identifiers and ownership are checked. A confirmed restriction may require lawful blocking, freezing, rejection or reporting. Assets must not be returned or converted in breach of a restriction. AYOV cannot remove a legal restriction by commercial agreement, and staff may be unable to disclose confidential reporting details.

Clients must provide truthful information and may supply reliable evidence to correct an erroneous match through Compliance. A screening result is not a general accusation of wrongdoing. Decisions and releases require recorded review. Using a new wallet, intermediary or chain to circumvent a restriction is prohibited.

# 6 Fraud prevention and complaints policy

AYOV will not ask for a recovery phrase or private key, or require an undisclosed “unlock fee” to validate a public transaction hash. Verify contract addresses and beneficiary details from the accepted documentation. Treat unsolicited guaranteed-return offers, urgent payment changes, remote-access requests and cloned websites as warning signs. A familiar display name or logo is not proof of authority.

If compromise or diversion is suspected, stop further instructions, protect the affected account/wallet through its genuine provider and contact compliance@ayovcapital.com promptly through an independently verified channel. Provide non-secret transaction references and relevant correspondence. Do not publicly post identity or bank records. Blockchain transfers may be irreversible; recovery is not guaranteed.

AYOV's required response is to register the case, contain affected access, preserve evidence, assess loss, coordinate with genuine providers and make required reports. Client communications must distinguish facts from estimates. Material incidents require management oversight and corrective testing. Confidentiality and legal restrictions may limit what can be disclosed during an investigation.

Complaints may be sent to compliance@ayovcapital.com with the service, relevant dates, reference and requested outcome. Do not include passwords. The internal service target is acknowledgement within five business days and a reasoned response within twenty business days, or an explanation and next update. Applicable legal or licence deadlines take precedence. Escalation rights and the responsible provider must be identified in the response; this policy does not claim membership of a compensation or ombudsman scheme.

# 7 Cookie and similar storage policy

The public AYOV website must offer two equally accessible choices when no valid preference is recorded: **Accept all cookies** and **Accept necessary cookies**. A persistent **Cookie settings** control must allow a later change. Necessary-only access must not be treated as acceptance of a transaction, marketing or investment agreement.

Strictly necessary storage supports essential functionality, security and remembering choices. Optional analytics and marketing technologies must remain disabled until valid consent where required. Consent must not be inferred from scrolling, continued browsing or a preselected optional box. Any new optional provider must be identified, classified and technically tested before activation.

The accompanying implementation stores a versioned preference named ayov_cookie_consent_v2 for up to 180 days. On HTTPS ayovcapital.com hosts it uses a first-party cookie scoped to ayovcapital.com so participating subdomains can read the same choice, with a local-storage fallback. The record contains the choice, version and dates, not a customer or payment credential. A shared choice applies only where the common consent control is installed; it does not prove that every subdomain has been updated. If storage is blocked, the site remains accessible but the choice may not persist. Optional categories default to off.

This policy does not itself prove that the implementation is live. The release must be verified on the homepage and subsidiary pages. The implementation must gate declared optional scripts and frames; staff must not install uncontrolled trackers outside that mechanism. Necessary security/account cookies on separate authenticated applications require their own inventory. Third-party links and wallet tools remain subject to

their own storage notices. Changing browser settings can remove stored choices and may make the banner reappear.

# 8 Product legal and risk disclosures

## Real asset tokens

The agreed token unit, issuer, asset entitlement, custodian, admitted reserve, evidence and redemption terms define the product. A report, CUSIP, allocation or asset valuation does not alone establish transferable title or immediate liquidity. An oracle provides a reference price; it does not inspect gold or guarantee a sale price. Published allocation, certified reserve and issued supply must be separately identified and dated.

Asset-backed tokens remain exposed to title, custody, fraud, insurance exclusions, valuation, market liquidity, legal enforcement and operational risks. Private/investment/trading labels do not determine regulatory classification. Client eligibility and transfer restrictions may limit liquidity. Redemption can involve notice, verification, minimum quantities, physical logistics and costs specified in the accepted terms.

## BOVEUR and vault routes

A BOVEUR institutional token using reserve certification and burn-to-cash processing is distinct from an ERC-4626 vault share. A vault accepts only its configured on-chain underlying asset. Clients must verify the full contract, chain, asset address, decimals, balances, eligibility rules and accepted product before sending anything. A similar symbol does not make two contracts interchangeable.

For an agreed ERC-4626 route, an approved holder authorises the underlying token and deposits through the vault method. Redemption burns shares and releases underlying according to the contract. Cash conversion is a separate accepted provider process. For an agreed burn-to-cash route, a confirmed burn is followed by the recorded payment process; a burn alone is not bank settlement. A custodian commitment hash is not a transaction receipt.

## Markets systems and rewards

Smart contracts may contain defects or privileged powers; networks may be delayed, congested or forked. Audits and verified source do not eliminate risk. Clients must understand actual pause, issuance, whitelist, recovery and administrative powers. Read-only explorer access requires no AYOV private key or server password.

Any client-reward programme must have a separate accepted schedule stating payer, eligibility, funding, calculation, caps, vesting, discretion, tax and cancellation treatment. There is no promise in this book of guaranteed income, appreciation or a redemption premium. Rewards must not be assumed to be funded by client backing. Product availability is subject to actual provider permissions and accepted terms, not the existence of a public page.

# 9 Policy administration

This book consolidates public policy language for the confirmed proposed business. The responsible entity must adopt and implement the policies, maintain records and identify the correct service provider at every

collection/contract point. Internal reporting procedures, monitoring configurations, officer personal details and confidential evidence are not public-policy content.

Policies are reviewed annually and after material change. The website must show current versions and preserve prior versions internally. A material change to accepted contractual rights follows the agreement and applicable law. Professional review must confirm licence scope, jurisdiction-specific privacy requirements and service agreements before regulated commencement; publication does not establish regulatory approval.