TITANIC MARKETS

BOARD-APPROVED GOVERNANCE POLICY

Financial Crime, AML/CTF and Sanctions Policy

A proportionate control framework for proprietary treasury operations.

> **Scope:** Titanic Markets OÜ invests and trades only its own corporate treasury. It does not hold, manage, transmit or trade assets for third parties and does not provide virtual-asset services to third parties. This policy therefore governs the company, its capital, counterparties, accounts, wallets and proprietary transactions—not a third-party onboarding programme.

LEGAL ENTITY
Titanic Markets OÜ

REGISTRY CODE / TIN
17525356

VERSION
1.0 — Public

EFFECTIVE DATE
15 July 2026

POLICY OWNER
Compliance Officer

REVIEW BY
15 July 2027

Document control

Legal entity	Titanic Markets OÜ, Estonian registry code 17525356
Registered office	Tööstuse tn 75-71, Põhja-Tallinna linnaosa, Tallinn, Harju maakond, 10416, Estonia
Document owner	Compliance Officer
Approval authority	Management Board
Approval evidence	Version-controlled publication authorised by the sole Management Board member
Version / classification	1.0 / Public
Effective / next review	15 July 2026 / no later than 15 July 2027
Contact	info@titanic-markets.com — subject: “Compliance”

Status and regulatory perimeter. This policy is voluntarily adopted as prudent corporate governance. It does not state or imply that Titanic Markets OÜ is a bank, financial institution, investment firm, crypto-asset service provider, obliged entity or licensed intermediary. The company must obtain written legal advice and update this framework before any activity could change that position. Applicable law overrides this policy.

1. Purpose and principles

Titanic Markets OÜ (“Titanic Markets” or the “company”) will not knowingly facilitate money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, corruption, tax crime or other misuse of the financial system. The purpose of this policy is to turn that commitment into controls proportionate to a young, owner-managed proprietary trading company.

Own treasury only

Every asset movement must have a documented corporate purpose and remain within the approved proprietary business model.

Know the source and destination

Capital provenance, account ownership, counterparties and wallet destinations must be understood before value moves.

Risk before speed

Uncertainty, sanctions concerns or unexplained activity pause a transaction. Commercial urgency never overrides a control.

Evidence over assertion

A control is treated as performed only when a dated record shows who did what, what was reviewed and what was decided.

The company applies a risk-based approach. Higher risk requires stronger evidence, senior approval, closer monitoring or refusal. A prohibition cannot be overridden merely by accepting higher risk.

2. Business model and policy scope

2.1 Current permitted model

- Investment and trading of the company's own corporate funds.
- Spot transactions in approved liquid crypto-assets and stablecoins through due-diligenced venues and company-controlled accounts.
- Corporate banking, custody, market-data, technology and professional services supporting that proprietary activity.
- Capital received transparently into the company under documented equity, shareholder or other board-approved arrangements.

2.2 Activities outside scope and prohibited without a change gate

The company must not commence any of the following unless section 13's change gate is completed:

- holding, safeguarding, managing, transmitting, exchanging or trading assets for a third party;
- operating an exchange, broker, payment, remittance, custody, lending, staking-as-a-service or pooled investment service;
- accepting deposits, executing third-party instructions, opening omnibus accounts or permitting pass-through activity;
- marketing a regulated financial or crypto-asset service; or
- any activity requiring authorisation, registration, an appointed MLRO or a statutory AML programme.

2.3 Instruments and leverage

Unless separately approved after documented legal and risk review, the treasury mandate is spot-only. Margin, leverage, derivatives, anonymous instruments and privacy-enhancing assets or services are outside the mandate.

3. Governance and accountability

3.1 Management Board

The Management Board owns financial-crime risk and must:

- approve this policy at adoption and at least annually;
- approve the enterprise risk assessment, risk appetite and material exceptions;
- ensure sufficient time, tools and professional advice are available;
- review material incidents and decide whether activity may resume; and
- ensure regulatory-perimeter review precedes any material business-model change.

3.2 Compliance Officer

The sole Management Board member is designated Compliance Officer until another suitably qualified person is formally appointed. The Compliance Officer has unrestricted access to company records and authority to stop onboarding of a capital source or counterparty, freeze an internal workflow, suspend a transfer or venue, preserve evidence, seek external advice and contact a competent authority.

The Compliance Officer maintains the policy, risk assessment, screening records, counterparty register, account and wallet inventory, exception log, training record, incident log and review calendar. Where the Compliance Officer is personally conflicted, external counsel or an independent professional must review the matter before action.

3.3 Segregation and single-person governance

The company acknowledges concentration risk while it has one officer. Compensating controls are mandatory: immutable venue and bank records, version-controlled policies, written pre-transaction rationale for material transfers, monthly reconciliations, out-of-band verification of settlement changes and independent review at the triggers in section 12. No document may claim dual approval while only one authorised officer exists.

4. Enterprise financial-crime risk assessment

The Compliance Officer must update the assessment at least annually and before a material product, asset, venue, jurisdiction, capital-source, custody or ownership change. Each assessment records inherent risk, controls, residual risk, owner, evidence, action and due date.

Risk area	Inherent risk	Core controls	Target residual risk
Capital provenance and ownership	Medium	Identity/ownership verification, source-of-funds and source-of-wealth evidence, sanctions/PEP/adverse-media review, company-account-only receipt.	Low–Medium
Crypto-asset transfers	High	Allowlisted destinations, ownership evidence, purpose record, custodial venues by default, blockchain analytics before non-custodial transfers.	Medium
Banks, exchanges and custodians	Medium–High	Regulatory-status checks, reputation and jurisdiction review, account ownership, security controls and periodic refresh.	Medium
Sanctions and geographic exposure	High	EU/UN/Estonian controls, event-driven screening, ownership/control analysis, dynamic jurisdiction register and escalation.	Medium
Spot proprietary trading	Medium	Approved asset/venue mandate, timestamped decision and order logs, position limits and reconciliation.	Low–Medium
Cyber compromise and fraud	High	MFA, least privilege, withdrawal controls, credential separation, verification of changed instructions and incident response.	Medium
Related-party or personal use	High	Corporate-purpose requirement, no personal wallets/accounts, conflict log, documentation and board record.	Low
Single-person governance	High	Evidence trail, reconciliation, external advice, independent review triggers and mandatory control redesign as staffing grows.	Medium

> **Overall target residual risk: Medium.** This is not acceptance of financial crime. It recognises the intrinsic risks of crypto-assets, cross-border venues and concentrated governance while requiring concrete mitigation and refusal where risk cannot be understood or controlled.

5. Risk appetite and prohibitions

The company has zero appetite for deliberate financial crime, sanctions evasion, concealment of ownership or misleading a financial institution. The following are prohibited:

- cash funding; bearer instruments; anonymous, fictitious, nominee or unverifiable funding;
- receiving funds from, or sending funds to, an account or wallet not demonstrably connected to the documented source, destination or corporate purpose;
- personal use of company accounts, wallets, credentials or venue access;
- shell banks, nested or pass-through accounts, unlicensed or unverifiable venues and counterparties that refuse ownership information;
- mixers, tumblers, peel chains or other deliberate obfuscation; privacy tools used to frustrate tracing; and transactions designed to bypass reporting, limits or screening;
- activity involving a person, entity, wallet, asset or transaction subject to a binding asset freeze or other applicable prohibition;
- false, incomplete or misleading statements to banks, venues, authorities, auditors or capital providers; and
- overriding a compliance stop without a dated written decision and, where needed, independent legal advice.

6. Capital provenance and ownership controls

Before accepting new capital, and before any material additional contribution, the company must create a capital-source file containing:

1. **Identity and authority.** Reliable identity information for a natural person; for a legal person, registry evidence, governing documents, authorised representative and signatory authority.
2. **Ownership and control.** Ultimate beneficial owners and persons exercising control, traced through each ownership layer with discrepancies resolved.
3. **Source of funds.** Evidence explaining the specific money or assets transferred, such as bank statements, audited accounts, transaction records, sale documents or tax records.
4. **Source of wealth.** Proportionate evidence explaining how the contributor accumulated overall wealth where the risk, amount, structure or PEP status requires it.
5. **Payment origin.** Proof that the remitting bank account or wallet is controlled by the documented contributor. Third-party payments require independent legal review and explicit board approval; anonymous payments are refused.
6. **Screening and geography.** Sanctions, PEP and risk-based adverse-media checks, plus assessment of residence, nationality, incorporation, banking and source jurisdictions.
7. **Decision.** A dated acceptance, enhanced-review or rejection record, with evidence references and the decision-maker.

Existing capital and ownership must be documented to this standard within ten business days of this policy’s adoption. Until the file is complete, the company must not represent that retrospective verification has been completed.

7. Counterparty and provider due diligence

Due diligence is required before opening or materially expanding a relationship with a bank, exchange, custodian, OTC desk, broker, lender, payment provider, corporate-service provider, technology vendor with asset access or other material counterparty.

Control	Minimum evidence
Legal existence and ownership	Official registry or equivalent evidence, registered address, operating website and material ownership/control information.
Regulatory status	Primary regulator or licence register where relevant; services and jurisdictions must match the authorisation.
Sanctions and integrity	Name and ownership/control screening, enforcement history, credible adverse media and unresolved warnings.
Financial-crime framework	Published policy, questionnaire, contractual warranties or other proportionate evidence where the counterparty handles money or assets.
Security and settlement	MFA, withdrawal/address controls, key-management model, incident history, contractual destination and change-verification process.
Decision and monitoring	Risk rating, approver, restrictions, evidence date and next review date.

High-risk counterparties are reviewed at least annually; others at least every two years. A material ownership, licensing, jurisdiction, service, enforcement, security or reputational event triggers immediate review. Failure to obtain sufficient information means the relationship does not start or is suspended.

8. Sanctions, PEP and adverse-media controls

8.1 Applicable and supplemental regimes

The company must comply with sanctions binding in Estonia, including applicable Estonian, European Union and United Nations measures. United States OFAC and United Kingdom OFSI measures are screened as supplemental risk controls and applied where a US/UK nexus, venue term, contractual obligation or other legal basis makes them relevant. Foreign measures must not be mischaracterised as Estonian law. OFAC measures are programme-specific; there is no single fixed list of “OFAC-sanctioned countries.”

8.2 Who and what is screened

- capital contributors and their beneficial owners, controllers, authorised representatives and relevant connected parties;
- material counterparties, providers, their relevant owners/controllers and settlement payees;
- known bank accounts, wallet addresses and destination identifiers linked to a material transfer; and
- countries, sectors, assets, services and transaction routes implicated by applicable restrictions.

8.3 Timing and method

Screening occurs before a relationship or capital contribution, before the first transfer, at periodic review, on a material trigger and promptly following a relevant sanctions event. Records include:

- the official or reputable source, list version/date, query terms and date/time;
- aliases, dates of birth, nationality, registration numbers, addresses and other identifiers sufficient to distinguish a true match;
- ownership and control analysis, not only exact-name matching; and
- the reviewer, result, evidence and disposition of every potential match.

Manual screening is permitted while volumes are low if evidence is retained. A commercial screening tool must be implemented before manual processes become unreliable. Non-custodial crypto transfers are prohibited until an appropriate blockchain-analytics check can be performed and retained; transfers between verified company accounts at due-diligenced custodial venues remain subject to destination and purpose controls.

8.4 Jurisdiction risk

The Compliance Officer maintains a dated jurisdiction register using current primary sources, including binding sanctions, FATF jurisdictions subject to a call for action or increased monitoring, EU high-risk third countries, corruption and secrecy indicators and the company's ability to verify ownership and funds. The register is dynamic; this public policy deliberately does not embed a list that can become stale.

8.5 Politically exposed persons

PEP status is not automatically a prohibition. A PEP, family member or known close associate requires documented enhanced review, stronger source-of-wealth and source-of-funds evidence, explicit board approval, annual review and heightened attention to credible adverse information.

8.6 Potential sanctions match

Do not transact, release, return or alert the affected party before review. Pause the action, preserve records, distinguish the identity using reliable identifiers, obtain legal advice where needed and comply without delay with any applicable freeze, prohibition and reporting duty. A false positive may be closed only with documented reasons.

9. Accounts, wallets and transfer controls

9.1 Inventory and ownership

The Compliance Officer maintains a confidential inventory of every bank account, venue account, wallet, public address, key/custody arrangement, authorised person, access method and business purpose. Only accounts and wallets in the company's name or demonstrably controlled for the company may be used. Personal accounts and wallets are prohibited.

9.2 Access security

- phishing-resistant MFA where available, unique credentials and least-privilege access;
- API keys limited by function and IP where supported, with withdrawals disabled unless specifically required;
- separation of trading, read-only and withdrawal permissions; no credentials shared through personal channels;
- quarterly access review and immediate revocation when access is no longer required; and
- secure backup and recovery tested proportionately to the custody model.

9.3 Transfer workflow

Every material transfer must have a record created before release containing amount/asset, source, destination, beneficial owner, business purpose, evidence, screening result, approver and transaction reference. New or changed settlement instructions require out-of-band verification using a trusted contact method.

While there is one authorised officer, the written pre-transfer record and later reconciliation are mandatory compensating controls. As soon as a second suitable authorised officer is appointed, material withdrawals and new allowlisted destinations require dual approval. Thresholds are recorded in the confidential treasury procedure and may only be changed by board decision.

9.4 Unexpected receipts

An unexpected third-party receipt is isolated and investigated. It is not automatically spent, traded, swept or returned, because a return could complete a laundering path or breach sanctions. The Compliance Officer documents the origin, legal basis, screening, advice and disposition.

10. Monitoring, escalation and reporting

10.1 Expected activity

Expected activity is limited to documented capital, treasury rebalancing, spot proprietary trading, operating expenses and legitimate investment or financing transactions approved by the board. Timestamped strategy, decision, order and execution logs provide the baseline for proprietary trading.

At least monthly, the Compliance Officer reviews and reconciles:

- bank, venue and wallet balances against the ledger;
- deposits and withdrawals against approved purposes and known destinations;
- new addresses, counterparties, users, API keys and permission changes;
- failed, reversed, unusual or manually overridden transactions; and
- open screening alerts, exceptions, incidents and remediation actions.

10.2 Red flags

- ownership, identity, purpose, source or destination cannot be explained or changes without credible reason;
- funds arrive from an unrelated person, opaque chain, high-risk route or recently created account;
- rapid pass-through movements, round-number splitting, repeated near-threshold activity or circular flows;
- use of obfuscation services, exposure to theft/ransomware/dark-market typologies or unexplained chain hopping;
- pressure to ignore controls, conceal a person, misdescribe a payment or bypass a venue restriction;
- adverse media, enforcement, licence loss, insolvency or control change affecting a counterparty; or
- account takeover indicators, changed settlement details, unusual devices or unexpected permission changes.

10.3 Escalation protocol

1. **Pause.** Stop the proposed action where operationally and legally possible.
2. **Preserve.** Secure logs, statements, communications, screening evidence and transaction identifiers.

3. **Investigate.** Establish facts, ownership, purpose, legal obligations and whether external expertise is required.
4. **Decide.** Record release, restriction, rejection, termination, freeze or other disposition and its rationale.
5. **Report.** Notify the Estonian Financial Intelligence Unit, law enforcement, a regulator or another competent authority without delay where a binding duty applies. Do not submit a report merely to create the appearance of compliance.
6. **Remediate.** Record root cause, control changes, owner and completion date.

> **No retaliation and no tipping-off.** A person raising a concern in good faith is protected from retaliation. Information about an investigation or report is disclosed only where authorised and must not be used to alert an affected person when doing so could prejudice a review or violate law.

11. Records, confidentiality and data protection

The company retains the evidence needed to reconstruct decisions and transactions for at least seven years from the later of the record date, transaction date or end of the relevant relationship, unless a longer period is required by law, litigation hold, investigation or contract. This baseline reflects Estonian accounting and tax record-retention requirements and applies to:

- identity, ownership, source-of-funds and source-of-wealth evidence;
- screening queries, results, false-positive decisions and jurisdiction assessments;
- counterparty approvals, contracts, regulatory checks and periodic reviews;
- bank, venue, wallet, blockchain, order, execution, reconciliation and accounting records;
- risk assessments, board approvals, policy versions, exceptions, incidents and reports;
- training materials, completion evidence and independent-review reports.

Records must be accurate, timestamped, retrievable, protected against unauthorised alteration and accessible only on a need-to-know basis. Personal data is limited to what is necessary, secured appropriately and deleted when the retention basis expires. A legal hold suspends deletion.

12. Training, testing and assurance

12.1 Training

The Compliance Officer must complete documented financial-crime and sanctions training within 30 days of adoption and at least annually thereafter. Any future person with treasury, accounting, access, approval or compliance duties must complete role-appropriate training before receiving access and annually. Training covers this policy, current typologies, sanctions, red flags, escalation, information security and relevant legal changes. Evidence includes the syllabus, material, date, provider, attendee and completion result.

12.2 Control testing

The Compliance Officer performs and records an annual self-assessment against this policy. An independent qualified reviewer must assess design and implementation at least every two years, and earlier before:

- the first external equity financing that introduces a new beneficial owner or complex capital source;
- material use of self-custody or non-custodial transfers;
- any activity potentially requiring financial or crypto-asset authorisation;

- a significant increase in transaction volume, geographic exposure or staffing; or
- resumption after a material financial-crime, sanctions, fraud or custody incident.

Findings are risk-rated, assigned an owner and due date, and tracked to evidenced closure. Until an independent review has actually occurred, the company must not attest that one has.

13. Change management, outsourcing and future structure

13.1 Regulatory change gate

Before a material new activity begins, the Management Board must obtain and retain:

1. a written description of the proposed service, users, funds flow, custody, jurisdictions and technology;
2. current legal advice on Estonian and EU regulatory classification, licensing, AML, sanctions, consumer, tax and data-protection duties;
3. all required authorisations or registrations before launch;
4. an updated enterprise risk assessment, policies, procedures, staffing, training, monitoring and assurance plan; and
5. a dated board go/no-go decision confirming that every prerequisite is evidenced.

13.2 Outsourcing

No component of the company's financial-crime framework is currently represented as outsourced. Before engaging a screening, blockchain-analytics, compliance, fund-administration or similar provider, the company assesses competence, security, data location, subcontracting, audit rights, resilience and exit arrangements. Outsourcing never transfers accountability from the Management Board.

13.3 Branches and subsidiaries

The company currently has no branches or subsidiaries. This policy applies automatically to any future controlled entity until a stricter local policy is approved. Before establishment, legal differences and the ability to apply group controls must be assessed.

14. Exceptions, breaches and review

A legal or sanctions prohibition cannot be waived. Any other exception must be rare, time-limited, documented before the activity, approved by the Management Board, supported by compensating controls and entered in the exception log. The record identifies the policy clause, reason, risk, control, owner, expiry and closure evidence.

A suspected breach is reported immediately to the Compliance Officer, preserved, investigated and remediated under section 10. Material breaches are recorded in board minutes and referred for external legal advice where appropriate.

This policy is reviewed at least annually and after a legal change, material new activity, ownership or governance change, significant incident, audit finding or control failure. The public version is updated promptly after approval. Confidential procedures, thresholds, wallet data, screening results and investigation records are not published.

Appendix A — Operating checklist

When	Required action	Evidence
On adoption	Complete retrospective capital/ownership file; account/wallet inventory; counterparty register; baseline risk assessment; initial screening; training within 30 days.	Dated registers, searches, decisions, training record.
Before new capital	Verify identity, ownership/control, authority, source of funds/wealth, payment origin, sanctions/PEP/adverse media and geography.	Capital-source file and approval.
Before a new provider	Verify existence, regulation, ownership/control, integrity, security, settlement and legal terms.	Counterparty file, rating and approval.
Before a material transfer	Confirm company purpose, source/destination ownership, screening, address/account, permissions and approval.	Pre-transfer record and transaction reference.
Monthly	Reconcile accounts/wallets/ledger; review deposits, withdrawals, access changes, exceptions and alerts.	Signed monthly control record.
On a trigger	Re-screen and reassess affected person, counterparty, jurisdiction, wallet, asset or activity.	Trigger review and disposition.
Quarterly	Review access, API keys, withdrawal rights, allowlists and inventory completeness.	Access-review record.
Annually	Policy/board approval, enterprise risk assessment, training, control self-assessment and high-risk reviews.	Board record, versions and completion evidence.
Every two years / trigger	Independent review under section 12.2.	Review report and remediation tracker.

Appendix B — Primary source hierarchy

The Compliance Officer verifies current requirements at the time of each decision. Consolidated lists and legal texts change; bookmarked or downloaded copies are not assumed current. Primary sources take precedence over press summaries and commercial databases.

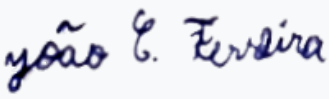
Subject	Primary source
Estonian law and consolidated acts	Riigi Teataja — riigiteataja.ee/en
Estonian sanctions and reporting guidance	Estonian Financial Intelligence Unit — fiu.ee/en
EU restrictive measures and resources	European Commission sanctions overview
EU consolidated financial-sanctions dataset	data.europa.eu consolidated list dataset
UN Security Council sanctions	UN Security Council consolidated list
FATF higher-risk jurisdictions	FATF monitored jurisdictions
US sanctions (supplemental / nexus-based)	OFAC Sanctions List Service and program information
UK sanctions (supplemental / nexus-based)	Office of Financial Sanctions Implementation

Management Board approval

By authorising version-controlled publication of this document, the sole Management Board member of Titanic Markets OÜ adopts version 1.0 with effect from 15 July 2026, designates the sole Management Board member as Compliance Officer and requires implementation of the time-bound actions stated in this policy.

Approving authority	Management Board, Titanic Markets OÜ
Approval mechanism	Signed and dated approval with version-controlled publication in the company's public website repository
Effective date	15 July 2026
Next review	No later than 15 July 2027

Signed for and on behalf of Titanic Markets OÜ



João Paulo Ramos Carrasco Ferreira
Sole Management Board Member & Compliance Officer

Signed: 15 July 2026
Effective: 15 July 2026
Version: 1.0 — Public