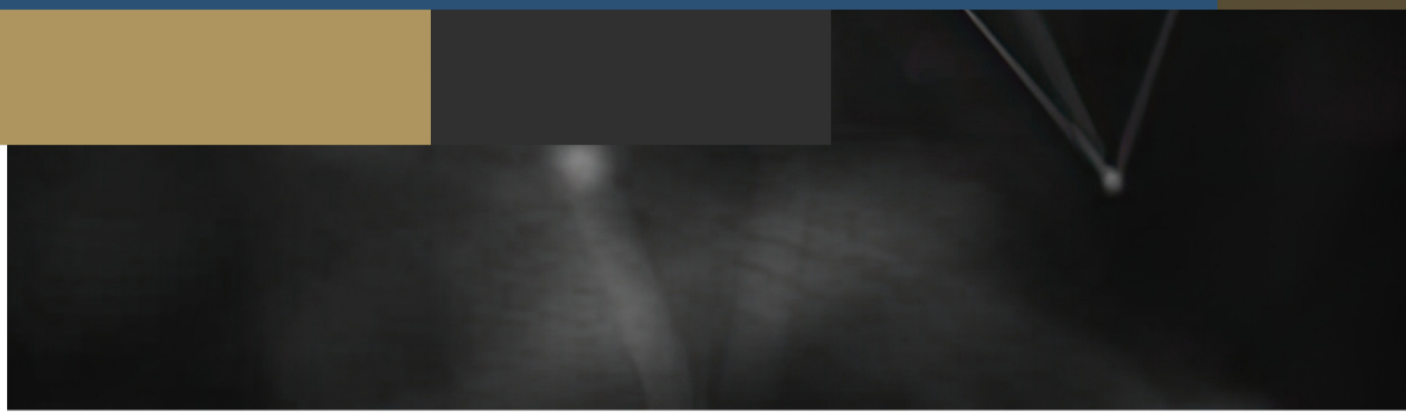
office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

AML CTF & SANCTIONS POLICY AND OPERATING STANDARDS



PRIVATE & CONFIDENTIAL

DO NOT COPY - NOT FOR DISTRIBUTION OR CIRCULATION

PRIVATE & CONFIDENTIAL

STICHTING ADMINISTRATIEKANTOOR S.P.A.F.

Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands

AML/CTF & Sanctions Policy and Operating Standards

Document type: Policy (institutional) with controlled annex procedures

Entity: Stichting Administratiekantoor S.P.A.F. ("S.P.A.F." or the "Foundation")

Perimeter (as instructed): (i) hybrid custody model (custodial + non-custodial/ client-controlled), (ii) counterparties restricted to professional investors/ qualified counterparties only, (iii) both fiat and digital-asset rails.

Effective Date: 3 March 2026

Version: 1.1 (fully revised)

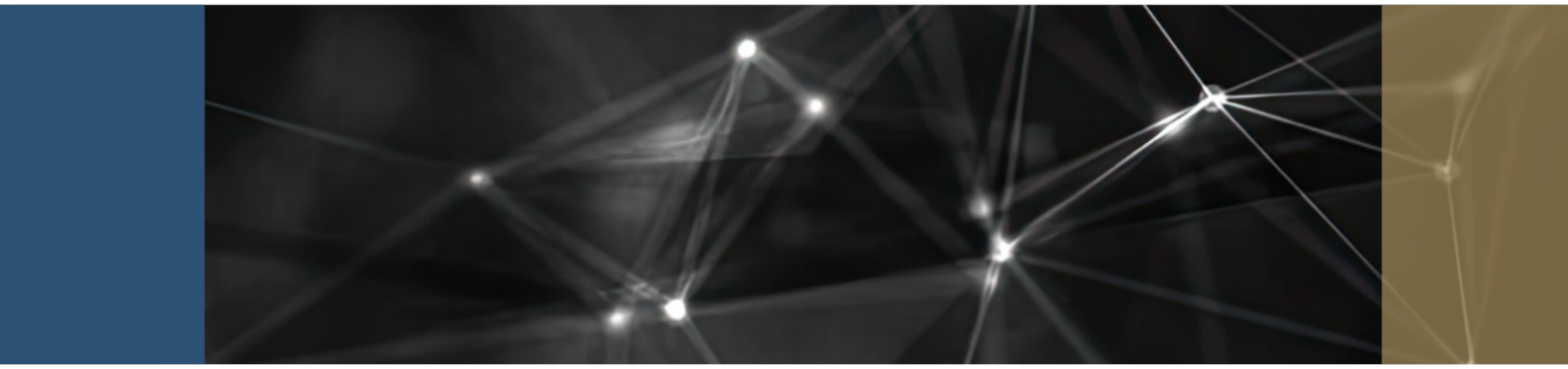
Owner: MLRO / Compliance Officer

Approver: Board of Directors

Review Cadence: At least annually and upon material change

Confidentiality: Internal / Restricted distribution

TABLE OF CONTENTS



office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

1. EXECUTIVE STATEMENT

S.P.A.F. maintains a financial crime compliance framework designed to prevent and detect money laundering, terrorist financing, sanctions violations and evasion, and associated predicate offenses (including fraud and corruption). The framework is risk-based, proportionate, auditable, and calibrated to S.P.A.F.'s operating perimeter: professional/qualified counterparties only, both fiat and digital-asset rails, and a hybrid custody posture where S.P.A.F. may, in certain structures, control investor assets and, in other structures, interact with client-controlled wallets.

This Policy establishes mandatory governance, due diligence standards, sanctions controls, transaction monitoring expectations, custody controls, escalation protocols, and record keeping requirements. It is written to be implementable by institutional operators, administrators, and regulated banking partners, and is supported by controlled annex procedures.

Incorporation and hierarchy. This Charter is to be read together with S.P.A.F.'s controlled governance and risk documents, including the **Enterprise-Wide Risk Assessment and Risk Appetite Statement** (*Annex A*), Delegation of Authority schedule, and Board Procedures Manual. Where this Charter conflicts with the Foundation's articles of association or mandatory law, the latter prevail. Where this Charter conflicts with annexed procedures, this Charter prevails unless the Board has expressly approved a derogation.

2. SCOPE AND APPLICABILITY

This Policy applies to the Board, directors, officers, employees, contractors, advisers, and any outsourced provider performing onboarding, dealing, treasury, custody, reconciliation, accounting, administration, or compliance functions on behalf of S.P.A.F. It covers all business relationships and transactions involving the receipt, holding, control, transfer, exchange, or disbursement of value, whether via bank rails or digital-asset rails, and whether under a custodial structure or a client-controlled wallet structure.

Where legal classification as an "**obliged entity**" for specific activities applies under Dutch/EU rules, S.P.A.F. will execute the additional duties that attach to that classification (including, where required, unusual transaction reporting to FIU-NL through the applicable process). Where a reporting duty does not attach to S.P.A.F. for a specific activity, S.P.A.F. will still operate to substantially equivalent institutional standards and will coordinate with regulated banking partners and counsel while preserving confidentiality and avoiding tipping-off.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

3. DEFINITIONS (OPERATIONAL)

For the purposes of this Policy, the following terms are used in their practical compliance meaning:

- **CDD / KYC / KYB:** customer/counterparty due diligence for individuals and legal entities, including verification and screening.
- **EDD:** enhanced due diligence is applied when risk is elevated, and standard controls are insufficient.
- **UBO:** ultimate beneficial owner(s) and controllers of an entity, through to natural persons.
- **PEP:** politically exposed person, including close associates and family members as applicable.
- **Sanctions:** applicable EU/UN and relevant national restrictive measures, including asset freezes and dealing prohibitions.
- **Custodial model:** structures where S.P.A.F. or its delegated custody function has control over assets/wallets or can effect transfers (directly or through controlled credentials/keys).
- **Non-custodial model:** structures where the investor/client controls the wallet credentials and S.P.A.F. interacts via pre-agreed addresses, operational attestations, and risk controls.
- **Travel rule information:** originator/beneficiary data elements required by regulated intermediaries for certain transfers; S.P.A.F. must support completeness when flows rely on regulated providers.

4. GOVERNANCE AND OPERATING MODEL

4.1 BOARD RESPONSIBILITY

The Board approves this Policy, sets financial crime risk appetite, and receives periodic reporting that allows it to exercise oversight. Oversight includes approval of material exceptions, review of significant incidents, and confirmation that remediation is completed.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

4.2 MLRO / COMPLIANCE OFFICER

The MLRO owns the framework and has the authority to halt onboarding, pause or reject transactions, impose risk conditions, and recommend relationship exit. The MLRO ensures implementation of screening, monitoring, escalation, and record keeping; maintains the EWRA; and ensures training and independent testing occur. In addition, the MLRO is the sole authorized decision maker for suspicion determinations and any external reporting decision that applies to S.P.A.F.

4.3 FIRST LINE (OPERATIONS, TREASURY, DEAL TEAMS, ADMINISTRATORS)

First line is accountable for collecting and validating due diligence data to the defined standard, ensuring payment and custody controls are applied as designed, executing monitoring reviews assigned to first line, and escalating red flags without delay.

4.4 INDEPENDENT ASSURANCE

Independent testing is conducted at least annually and covers onboarding completeness, screening performance, monitoring effectiveness, custody controls (*where applicable*), and the quality of escalation decisions and audit trail.

5. RISK-BASED APPROACH AND RISK APPETITE

S.P.A.F. maintains an enterprise-wide financial crime risk assessment that informs onboarding standards, approval thresholds, monitoring rules, custody controls, and training. The Foundation's appetite is restrictive with respect to opacity, sanctions risk, unexplained third-party funding, and high-risk typologies common to digital-asset misuse.

S.P.A.F. will not proceed where identity/UBO cannot be verified to a reasonable institutional standard, where sanctions exposure exists, where the relationship appears designed to conceal ownership or origin of funds, where the counterparty will not provide required evidence, or where risk cannot be reduced to within appetite through EDD and structural controls.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

6. COUNTERPARTY ELIGIBILITY PERIMETER: PROFESSIONAL INVESTORS / QUALIFIED COUNTERPARTIES ONLY

All relationships in scope must be with professional investors and/or qualified counterparties. This is implemented as a formal eligibility gate in onboarding: S.P.A.F. documents the classification basis, obtains written representations, and retains corroborating evidence proportionate to the jurisdictional regime and the counterparty profile. Any relationship that cannot be classified and evidenced to the required standard is declined. The eligibility gate is not a formality; it is a control that limits mis-selling, reduces consumer-harm exposure, and supports the risk-based perimeter of this Policy.

(See Annex B for the controlled procedure and template language.)

7. DUE DILIGENCE STANDARD (CDD) AND ONBOARDING REQUIREMENTS

7.1 ONBOARDING PRINCIPLE

No relationship is activated, no assets are accepted into custody, and no transaction is executed until onboarding is complete to the defined file standard and approved at the appropriate level.

7.2 MINIMUM CDD FOR INDIVIDUALS (WHERE RELEVANT)

S.P.A.F. verifies identity and address, screens sanctions and PEP/adverse media, documents the purpose and expected activity profile, and obtains source of funds evidence. Where risk warrants (including PEP or high value), the source of wealth is corroborated.

7.3 MINIMUM KYB FOR LEGAL ENTITIES

S.P.A.F. verifies legal existence, governance, directors and authorized signatories, and identifies and verifies UBOs and controllers through to natural persons. Ownership/control chains that are layered, use nominee arrangements, involve trusts/foundations, or rely on offshore jurisdictions require additional corroboration and an explicit economic rationale. The expected activity profile must specify flows (volumes, frequency), jurisdictions, rails, and intended counterparties.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

7.4 SOURCE OF FUNDS AND SOURCE OF WEALTH

S.P.A.F. requires evidence that is commensurate with the relationship's size and risk. Evidence must support plausibility, not merely existence. Where evidence is incomplete, but risk is moderate, S.P.A.F. may restrict the relationship to limited activity pending completion; where risk is high, S.P.A.F. will not proceed.

7.5 RELIANCE ON INTRODUCERS AND THIRD PARTIES

Reliance is permitted only where S.P.A.F. has conducted due diligence on the third party, has an enforceable contract setting standards and audit rights, and receives the full due diligence pack prior to activation. Reliance does not transfer accountability. (See Annex H.)

(See Annex C for file standard, completeness, and approval thresholds.)

8. ENHANCED DUE DILIGENCE (EDD) AND SENIOR APPROVALS

EDD is mandatory when risk is elevated due to counterparty profile, geographic exposure, structure opacity, adverse media, PEP exposure, third-party funding, or transaction behavior inconsistent with the expected profile, including elevated digital-asset typologies.

EDD includes: senior approval by the MLRO (and Board delegate when material), corroborated source of wealth, strengthened contractual and payment controls, restricted rails where appropriate, and a defined enhanced monitoring plan. If residual risk remains outside appetite, the relationship is declined or exited.

The Committee reviews the EWRA methodology, key assumptions, and remediation plan as set out in Annex A, and makes recommendations to the Board.

9. SANCTIONS COMPLIANCE (Screening, Investigation and Disposition)

S.P.A.F. screens counterparties, UBOs, directors, authorized signatories, relevant intermediaries, and (where applicable) beneficiaries and project partners at onboarding, prior to payment execution, periodically thereafter, and when trigger events occur (ownership changes, new jurisdictions, new counterparties, material changes in activity).

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

Potential matches cause an immediate pause of activation or payment execution pending a documented investigation by Compliance. True matches result in controlled actions consistent with legal requirements, including restrictions on dealing and any notifications/escalations required. Screening results and dispositions are retained as part of the audit trail.

(See Annex D.)

10. TRANSACTION MONITORING, INVESTIGATIONS, AND CASE MANAGEMENT

S.P.A.F. maintains ongoing monitoring calibrated to the relationship's expected activity profile and the custody model. Monitoring combines automated and manual controls and produces a documented case record for all material alerts. Monitoring is designed to identify inconsistent economic purpose, third-party funding, structuring behavior, rapid in-and-out flows, frequent instruction changes, high-risk corridor exposure, and digital-asset typologies associated with obfuscation or illicit sources.

Where digital assets are involved, S.P.A.F. applies additional controls appropriate to the custody model, including address verification and restriction, exposure assessment using fit-for-purpose tooling or regulated service providers, and controls to ensure travel-rule completeness where the flow relies on regulated intermediaries.

(See Annex E.)

11. CUSTODIAL VS. NON-CUSTODIAL CONTROLS (Mandatory Structural Discipline)

11.1 CUSTODIAL MODEL CONTROLS

Where S.P.A.F. has custody or control, S.P.A.F. applies institutional safeguarding controls: segregation of duties, dual authorization for movements, strict whitelisting of destination accounts/wallets, controlled change management for beneficiary details, secure key/credential management with access logging, and reconciliations that support asset integrity and traceability. Exceptions are rare, time-bound, and MLRO-approved with documented rationale.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

11.2 NON-CUSTODIAL MODEL CONTROLS

Where the client controls the wallet, S.P.A.F. treats control risk as higher unless mitigated through evidence and restrictions. S.P.A.F. requires evidence linking the counterparty to the wallet(s), restricts operational interaction to pre-verified addresses where feasible, increases scrutiny for address changes and third-party deposits, and applies enhanced monitoring triggers for behavioral variance relative to the expected activity profile.

(See Annex G.)

12. SUSPICION ESCALATION, REPORTING POSTURE, AND CONFIDENTIALITY

All personnel and service providers are required to escalate red flags promptly to the MLRO using the internal suspicion reporting procedure. The MLRO determines whether suspicion exists and records the decision, rationale, and instructions. Where statutory reporting applies, the MLRO ensures reports are made through the proper channel and maintains confidentiality and non-tipping-off controls. Where statutory reporting does not apply to S.P.A.F. for a specific activity, the MLRO still documents the assessment and coordinates with counsel and regulated banking partners as appropriate, preserving confidentiality.

(See Annex F.)

13. RECORDKEEPING, RETENTION, AND DATA PROTECTION

S.P.A.F. retains complete and searchable records supporting onboarding, screening, monitoring, custody operations (*where applicable*), and escalation decisions, with access controlled on a least-privilege basis. Records are retained for periods consistent with applicable legal requirements and institutional expectations for AML/sanctions audit trails, including post-termination retention sufficient to evidence compliance and support lawful inquiries. Personal data is handled in accordance with GDPR principles, and access to AML files is restricted and logged.

14. TRAINING AND COMPETENCE

S.P.A.F. delivers induction and annual training to all relevant personnel and service providers. Training is calibrated to S.P.A.F.'s perimeter and includes custody/non-custody controls, digital-asset typologies, sanctions basics, red flags, and escalation mechanics. Training completion and effectiveness are recorded. Remedial training is delivered when control failures occur.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

15. OUTSOURCING, THIRD-PARTIES, AND INTRODUCERS

Where S.P.A.F. relies on third parties for onboarding, administration, custody support, analytics, or introduction of counterparties, S.P.A.F. performs due diligence, contracts enforceable minimum standards (including audit rights and data delivery SLAs), and conducts ongoing oversight. Outsourcing does not reduce S.P.A.F.'s accountability.

(See Annex H.)

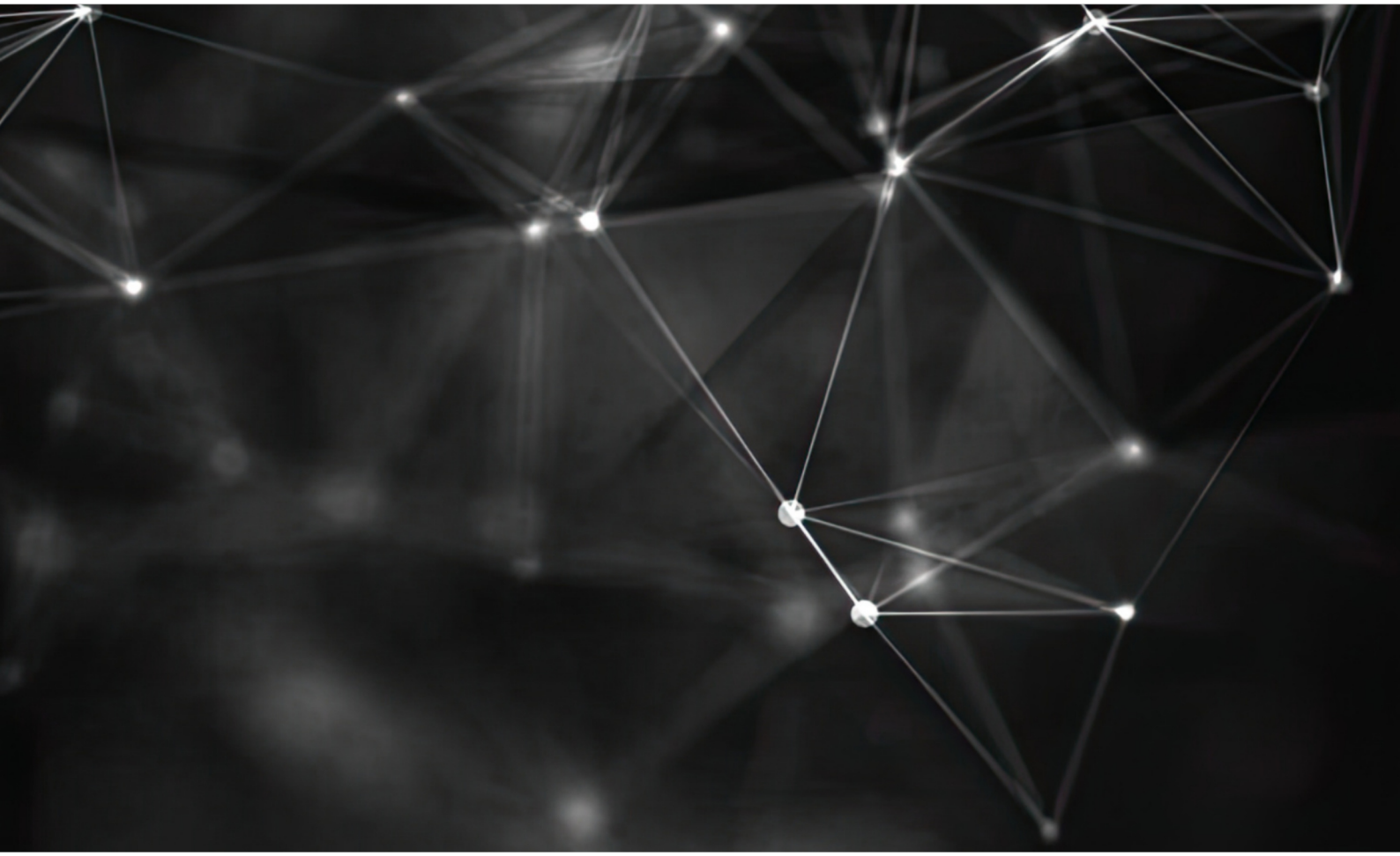
16. EXCEPTIONS, BREACHES, AND REMEDIATION

Any exception to this Policy must be documented, risk-assessed, time-bound, and approved by the MLRO; material exceptions require Board delegate approval. Policy breaches are recorded as incidents, investigated, remediated with defined owners and deadlines, and reported to the Board through periodic MI.

17. MANAGEMENT INFORMATION AND BOARD REPORTING

The MLRO provides periodic reporting to the Board (or delegated committee) addressing: onboarding volumes and risk ratings, EDD volumes, screening hits and dispositions, monitoring alert volumes and outcomes, custody control exceptions, incidents, remediation status, and any significant emerging risks.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org



ANNEXES

(CONTROLLED PROCEDURES & TEMPLATES)

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

ANNEX A — ENTERPRISE-WIDE RISK ASSESSMENT (EWRA) AND RISK APPETITE STATEMENT

Document Type: Procedure + Standard

Owner: MLRO | **Approver:** Board | **Frequency:** Annual + Event-Driven Refresh

A1. PURPOSE

To identify, assess, and document S.P.A.F.'s inherent and residual financial crime risks and to ensure controls and risk appetite remain aligned to the operating perimeter.

A2. METHOD

The EWRA evaluates five dimensions and records inherent risk, control strength, and residual risk. The dimensions are: counterparty risk (including professional-only perimeter enforcement), geographic risk, product/channel risk (including custody vs non-custody), transaction behavior risk, and sanctions risk. The EWRA must explicitly address digital-asset exposure and custody architecture, including key management and transfer authorization controls.

A3. OUTPUTS AND GOVERNANCE

The MLRO produces an EWRA report and a control improvement plan. The Board approves the EWRA and risk appetite statement. Where residual risk is above appetite, the activity is paused pending remediation or discontinued.

A4. RISK APPETITE STATEMENT (TEMPLATE)

S.P.A.F. maintains a low appetite for opacity and evasion risk. S.P.A.F. will not accept relationships where UBO/control cannot be verified, where the source of funds/wealth is not plausible, where sanctioned exposure exists, or where third-party funding is unexplained. S.P.A.F. maintains a cautious appetite for digital-asset flows and permits them only where traceability, screening, and monitoring controls are demonstrably effective and where custody controls meet institutional standards.

A5. RECORDS

EWRA report, risk appetite statement, Board approval minutes, and remediation tracker.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

ANNEX B — PROFESSIONAL INVESTOR / QUALIFIED COUNTERPARTY ELIGIBILITY PROCEDURE

Document Type: Procedure + Eligibility Memo Template

Owner: Compliance | **Approver:** MLRO | **Mandatory gate:** Yes

B1. STANDARD

S.P.A.F. engages only with counterparties that qualify as professional investors and/or qualified counterparties. Eligibility must be determined and documented prior to activation.

B2. PROCEDURE

Compliance collects a signed representation from the counterparty confirming professional/ qualified status and obtains corroborating evidence proportionate to the jurisdiction and counterparty type (regulated firm evidence, professional investor certification, institutional status documentation, or other defensible basis). Compliance records the classification basis in an Eligibility Memo that is stored with the onboarding file.

B3. TEMPLATE: ELIGIBILITY MEMO (MINIMUM FIELDS)

Counterparty legal name; jurisdiction; classification basis; evidence reviewed; any conditions or limitations; approver name/date; link to onboarding file.

B4. EXCEPTIONS

No exceptions. If classification cannot be documented, onboarding is declined.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

ANNEX C — CDD/EDD FILE STANDARD AND APPROVAL MATRIX

Document Type: Standard + Procedure

Owner: Compliance | **Approver:** MLRO

C1. "COMPLETE FILE" STANDARD

A file is complete only when it contains (i) verified identity/legal existence, (ii) verified UBO/control to natural persons, (iii) screening results (sanctions, PEP, adverse media) with disposition, (iv) purpose and expected activity profile, (v) source of funds evidence proportionate to risk, and (vi) professional investor eligibility memo.

For custodial relationships, the file must also include the custody model designation, destination whitelists, authorization matrix, and key management/control statements or attestations applicable to the structure.

C2. EDD REQUIREMENTS

EDD files must additionally include source of wealth corroboration, an enhanced monitoring plan, and senior approval documentation.

C3. APPROVAL MATRIX (INSTITUTIONAL STANDARD)

Low/Standard Risk: Compliance approval.

Medium Risk: MLRO approval.

High Risk: MLRO + Board delegate approval, plus EDD and enhanced monitoring plan as mandatory conditions.

Sanctions Match: activity paused; only MLRO may disposition; true match results in controlled actions and escalation to counsel.

C4. RECORDS

CDD checklist completion log; EDD pack; approvals; monitoring plan; restrictions.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

ANNEX D — SANCTIONS SCREENING AND HIT HANDLING SOP

Document Type: SOP

Owner: Compliance | **Approver:** MLRO

D1. SCREENING POINTS

Screening is performed at onboarding, prior to payment execution, periodically (defined by risk), and at trigger events. Screening covers counterparties, UBOs, controllers, directors, signatories, and relevant intermediaries. Where relevant, screening extends to beneficiaries and project partners.

D2. HIT HANDLING

When a potential match occurs, the transaction/onboarding is paused. Compliance performs identity resolution using available identifiers, assesses ownership/control, and documents the rationale for false positives or true matches. Only the MLRO can clear a true-risk hit. Any restriction is applied before further activity.

D3. CONTROLS

Screening evidence must be retained; screening tools must be validated and access controlled; disposition decisions must be documented with supporting evidence and approver.

D4. RECORDS

Screening logs; case notes; disposition memo; approvals; counsel escalation notes (if applicable).

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

ANNEX E — TRANSACTION MONITORING AND CASE MANAGEMENT STANDARD

Document Type: Standard + SOP

Owner: MLRO | **Operator:** Compliance + Designated First Line

E1. MONITORING BASELINE

Monitoring is anchored to the expected activity profile set at onboarding and adapted when the profile changes. Monitoring must reflect the custody model and the rails used. Rules are calibrated by risk rating and include behavioral indicators, not only thresholds.

E2. TRIGGER CATEGORIES (INSTITUTIONAL FRAMING)

Monitoring focuses on deviations from plausible economic purpose, third-party funding not consistent with profile, structuring behavior, rapid movement patterns, frequent instruction changes, high-risk corridor exposure, and digital-asset obfuscation indicators. Where regulated intermediaries are used, incomplete or inconsistent originator/beneficiary information is treated as a monitoring trigger.

E3. CASE HANDLING

Each alert becomes a case with a unique reference. Case files must contain: transaction facts, contextual profile, documents reviewed, analysis performed, decision outcome, approver, and rationale. Cases are closed only when the risk is addressed through clearance, restriction, escalation, or exit.

E4. RECORDS AND MI

Case register; alert volumes; outcomes; average time to closure; recurring themes; rule tuning log.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

ANNEX F — INTERNAL SUSPICION REPORTING AND MLRO DECISION PROCEDURE

Document Type: SOP + Template

Owner: MLRO | **Mandatory:** Yes

F1. ESCALATION REQUIREMENT

Any staff member or provider who identifies red flags must escalate immediately through the Internal Suspicion Report ("ISR"). Silence, delay, or informal handling is prohibited.

F2. ISR TEMPLATE (MINIMUM FIELDS)

Reporter identity; date/time; counterparty identifiers; transaction identifiers; narrative of concern; supporting documents; immediate risk actions taken (if any); recommended next step.

F3. MLRO DECISIONING

The MLRO reviews the ISR, requests additional information if needed, determines whether suspicion/unusual activity exists, and records the decision and rationale. Where statutory reporting applies, the MLRO ensures reporting is performed via the appropriate channel. Where statutory reporting does not apply to S.P.A.F. for the activity, the MLRO documents the decision and coordinates with counsel and regulated partners, preserving confidentiality.

F4. CONFIDENTIALITY AND TIPPING-OFF

Information about suspicion and any reporting decision is restricted to need-to-know. Communications with counterparties are controlled and must not imply that a report is contemplated or has been made.

F5. RECORDS

ISR log; MLRO decision log; reporting file (if applicable); counsel escalation notes.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

ANNEX G — CUSTODY, WALLET CONTROL, AND ASSET MOVEMENT STANDARD

Document Type: Standard + Control Requirements

Owner: COO/Treasury + MLRO (joint) | **Approver:** Board delegate for architecture changes

G1. CUSTODIAL MODEL (S.P.A.F.-CONTROLLED)

S.P.A.F. implements dual control for movements, strict whitelisting of destinations, controlled change management for beneficiary details, and credential/key management standards that enforce least privilege, access logging, and separation of duties. Reconciliations must demonstrate asset integrity daily (or more frequently where activity requires). Emergency procedures exist but are time-bound and require MLRO approval, with post- incident review.

G2. NON-CUSTODIAL MODEL (CLIENT-CONTROLLED)

S.P.A.F. requires evidence that links the counterparty to the wallet(s) used in the relationship, controls address changes through documented verification steps, and restricts interaction to pre-verified addresses where feasible. Third-party deposits into the relationship are treated as a risk event and require MLRO review unless pre- approved and justified in the expected activity profile.

G3. ASSET MOVEMENT GOVERNANCE

All movements have a documented business purpose, traceable authorization, and independent verification. Where digital assets are used, transaction hashes and on-chain evidence are retained in the case file and reconciliation record. Where fiat rails are used, bank confirmations and payment instructions are retained.

G4. RECORDS

Whitelist register, authorization logs, reconciliation logs; exception register; incident reports.

office@spaf-foundation.org
Gebouw Delftse Poort, Weena 505
3013 AL Rotterdam | The Netherlands
www.spaf-foundation.org

ANNEX H — THIRD-PARTY, ADMINISTRATOR, CUSTODIAN, AND INTRODUCER OVERSIGHT STANDARD

Document Type: Standard + Minimum Contractual Clauses

Owner: COO + MLRO | **Approver:** MLRO

H1. DUE DILIGENCE STANDARD

Prior to engagement, S.P.A.F. completes due diligence on third parties that support onboarding, administration, custody, analytics, or client introduction. Due diligence covers ownership, reputation, regulatory posture (where relevant), operational capability, information security, subcontracting, and financial stability.

H2. CONTRACTUAL MINIMUMS (INSTITUTIONAL CLAUSES, HIGH LEVEL)

The agreement must include confidentiality, GDPR/data processing provisions, minimum AML/sanctions standards consistent with this Policy, defined deliverables and SLAs for data provision, audit rights (including file sampling), subcontractor controls, incident notification obligations, and termination rights for compliance failures.

H3. ONGOING OVERSIGHT

S.P.A.F. performs periodic performance and compliance reviews, including file testing where onboarding is delegated and operational control testing where custody functions exist. Material findings trigger remediation plans with deadlines or termination.

H4. RECORDS

Vendor/introducer due diligence pack; contract; oversight reviews; issue logs; remediation tracker.