Sentu

AML & COMPLIANCE POLICY

Anti-Money Laundering · Counter-Terrorism Financing · Sanctions Compliance

Versión: v1.0 — March 2026

Colombia · United States · United Arab Emirates

SENTU'S COMMITMENT TO FINANCIAL INTEGRITY

Sentu Services operates a zero-tolerance policy against money laundering, terrorist financing, and sanctions evasion. We apply a risk-based approach aligned with FATF Recommendations, Colombian SARLAFT regulations, U.S. Bank Secrecy Act standards, and UAE Federal Law No. 20 of 2019.

01 SCOPE & APPLICABILITY

Who this policy covers

1.1 Entities Covered

This AML & Compliance Policy applies to all entities operating under the Sentu Services brand:

Entity	Jurisdiction	Applicable AML Framework
Sky OTC S.A.S.	Colombia	SARLAFT (Circular 100-000016/2021 Supersociedades) + UIAF reporting (Ley 526/1999)
Payki S.A.S.	Colombia	SARLAFT + SuperFinanciera guidelines for payment processors (SEDPE)
Sky Pay LLC	Montana, U.S.A.	Bank Secrecy Act (BSA) + FinCEN guidance + OFAC regulations
Sentu Services FZCO	Dubai, UAE	UAE Federal AML Law No. 20/2019 + CBUAE guidelines + goAML reporting

1.2 Persons Covered

This policy applies to: all employees, contractors, and agents of Sentu; all third-party service providers (payment rails, KYC vendors); all commercial brokers (agents) operating under a Sentu referral agreement; and all customers and users of the Sentu platform.

02 RISK-BASED APPROACH

How Sentu assesses and manages AML risk

2.1 Risk Philosophy

Sentu applies a risk-based approach (RBA) as defined by FATF Recommendation 1. This means we allocate compliance resources proportionally to the identified level of risk, applying enhanced measures to higher-risk situations and simplified (but never zero) measures to lower-risk ones.

2.2 Risk Factors Assessed

Risk Dimension	High Risk Indicators	Mitigation
Customer Risk	PEP (Politically Exposed Person); Sanctioned jurisdiction; Unusual wealth profile; Complex corporate ownership; Prior SAR history.	Enhanced Due Diligence (EDD); Senior management approval; Ongoing monitoring.
Geographic Risk	Transactions involving FATF high-risk jurisdictions; Offshore financial centers; Jurisdictions with weak AML controls.	Restrict or prohibit transactions; Apply EDD; Obtain source-of-funds documentation.
Product / Service Risk	Large single payments (>USD 50,000); Multiple rapid transactions; Unusual payment patterns; Payments inconsistent with investment profile.	Real-time transaction monitoring; Threshold alerts; Manual review queue.
Channel Risk	Anonymous registration attempts; Use of VPN/proxy to access platform; Unverified third-party brokers.	Mandatory KYC before any transaction; Broker verification program; Device fingerprinting.

2.3 Customer Risk Rating

Risk Level	Profile	Measures Applied
LOW	Verified individual; Colombian/Colombian resident; Clear source of funds; <USD 20,000 per transaction; No PEP; No adverse media.	Standard CDD. Annual KYC refresh.
MEDIUM	Foreign national from standard jurisdiction; Corporate client with transparent ownership; Transactions USD 20,000-100,000; No adverse indicators.	Standard CDD + annual verification. Source of funds required for each transaction >USD 20,000.
HIGH	PEP or PEP close associate; Transactions >USD 100,000; Complex ownership structure; Jurisdiction with elevated risk; Inconsistent financial profile.	EDD: senior management approval, enhanced documentation, quarterly review.
VERY HIGH / PROHIBITED	OFAC/UN sanctioned individual or entity; Jurisdiction under comprehensive sanctions; Prior confirmed SAR activity; Falsified KYC documents.	Refuse service. File SAR/STR if applicable. No exceptions.

03 CUSTOMER DUE DILIGENCE (CDD/EDD)

Know Your Customer procedures

3.1 Standard Customer Due Diligence (CDD) — Individuals

- Full legal name as per government-issued ID.
- Date of birth and nationality.
- Residential address (verified with recent utility bill or bank statement, max 90 days).
- Source of funds declaration (signed statement identifying the legal origin of the funds to be invested).
- Politically Exposed Person (PEP) self-declaration.
- Screening against OFAC SDN List, UN Consolidated Sanctions List, Interpol, UIAF Colombia national lists, and UAE Central Bank lists.
- Risk assessment and classification before onboarding.

3.2 Standard CDD — Legal Entities (KYB)

- Certificate of incorporation or equivalent (max 90 days validity).
- Constitutional documents (bylaws/articles of incorporation).
- Identification of all UBOs (Ultimate Beneficial Owners): individuals owning or controlling ≥25% directly or indirectly.
- Identification and KYC of legal representative(s).
- Corporate source of funds declaration.
- Most recent audited financial statements (for transactions >USD 100,000).
- AML compliance certification for entities with transactions >USD 200,000.

3.3 Enhanced Due Diligence (EDD)

EDD is applied to HIGH and VERY HIGH risk customers, and in addition:

- Transactions with counterparties in FATF-listed high-risk jurisdictions.
- Transactions where the customer is a PEP or close associate of a PEP.
- Transactions above USD 100,000 or patterns suggesting layering.
- Any situation where the source of funds is unclear or inconsistent with the customer's known profile.

EDD measures include: senior management written approval, additional documentation of wealth source (e.g., property deeds, business registration, share certificates), third-party verification of beneficial ownership, and more frequent transaction monitoring.

3.4 Ongoing Monitoring & KYC Refresh

Risk Level	KYC Refresh Frequency	Trigger for Immediate Review
LOW	Every 3 years	Adverse media; Unusual transaction pattern; Change of country of residence.
MEDIUM	Every 2 years	Same as above + transaction volume doubling without explanation.

Risk Level	KYC Refresh Frequency	Trigger for Immediate Review
HIGH	Every year	Any anomaly; New beneficial owner; Transaction >USD 50,000.
VERY HIGH	Every 6 months OR continuous	Any transaction; Any change in profile.

04 TRANSACTION MONITORING

Detecting suspicious activity

4.1 Monitoring Framework

Sentu monitors all transactions processed through its platform in real time. The monitoring system flags transactions based on the following rules, which are reviewed and updated quarterly:

4.2 Red Flags / Alert Indicators

Category	Indicator	Action
Unusual Amounts	Single payment >USD 100,000 from a customer with LOW risk rating.	Manual review + EDD if not explained.
Pattern	Multiple payments just below threshold (e.g., 3 x $9,500 in 48 hours — structuring).	SAR filing + account review.
Geographic	Payment originating from or going to a sanctioned jurisdiction.	Block transaction + SAR filing.
Identity	Customer uses multiple accounts with different IDs; Inconsistent IP/device location.	Flag for MLRO review. Potential account freeze.
Refusal to Provide Info	Customer declines to provide source of funds or KYC documentation when requested.	Refuse service + file SAR if there is reasonable suspicion.
Third-Party Payments	Payment on behalf of a customer originates from an unrelated third-party account.	Obtain written explanation. Block if not satisfactorily explained.
Inconsistent Profile	Investment amount disproportionate to declared income or financial profile.	Request additional documentation. MLRO decision.
Cash / Crypto Conversion	Indication that investment funds originated from cash or crypto without verifiable trail.	EDD + MLRO approval required.

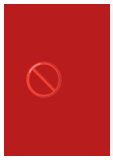
05 SANCTIONS COMPLIANCE

OFAC · UN · EU · UAE

Sentu maintains a zero-tolerance policy for transactions involving sanctioned individuals, entities, or jurisdictions. Sentu screens all customers, brokers, constructoras, and counterparties against:

- OFAC SDN (Specially Designated Nationals) List — U.S. Treasury.
- UN Security Council Consolidated Sanctions List.
- EU Consolidated Sanctions List.
- UAE Central Bank sanctions and Terrorism Financing lists.
- UIAF Colombia national lists and Policía Nacional.
- Interpol Red Notices (for high-risk situations).

Screening is performed at onboarding and on an ongoing basis (real-time for each transaction and batch screening at least weekly). Any positive match triggers immediate transaction blocking and MLRO notification within 24 hours.



Sentu does not process transactions from or to: Iran, North Korea, Syria, Cuba (sanctioned activities), Russia/Belarus (for restricted assets), or any other jurisdiction under comprehensive OFAC or UN sanctions. Violations of this policy may result in criminal liability for the individuals involved.

06 SUSPICIOUS ACTIVITY REPORTING (SAR/STR)

Reporting obligations

Jurisdiction	Report Type	Authority	Trigger Threshold	Deadline
Colombia	Reporte de Operación Sospechosa (ROS)	UIAF (Unidad de Información y Análisis Financiero)	No monetary threshold — based on suspicion	Within 24 hours of detection
Colombia	Reporte de Ausencia de Operaciones (RAO)	UIAF	When no transactions occur in a period for high-risk customers	Monthly
U.S.A.	Suspicious Activity Report (SAR)	FinCEN (Financial Crimes Enforcement Network)	USD 5,000 (for MSBs) if suspicious activity is involved	30 calendar days from detection

Jurisdiction	Report Type	Authority	Trigger Threshold	Deadline
UAE	Suspicious Transaction Report (STR)	Financial Intelligence Unit (FIU) via goAML	No monetary threshold — based on suspicion	Within 24 hours for terrorism financing; reasonable time for others

6.1 Tipping-Off Prohibition

⚠ It is strictly prohibited to inform a customer or any third party that a SAR/STR/ROS has been filed or is being contemplated. Violation of this prohibition may result in criminal liability. This prohibition applies to all employees, agents, and contractors of Sentu.

07 RECORD KEEPING

Data retention for AML purposes

Record Type	Retention Period	Format
KYC documentation (ID, proof of address, source of funds)	10 years from end of relationship	Secure digital archive, encrypted
Transaction records (amounts, dates, parties, routes)	10 years from date of transaction	Immutable digital record + backup
SAR/STR/ROS filings and supporting documentation	10 years from filing date	Separate secure archive, MLRO access only
Sanctions screening results	5 years	Digital log with timestamp
Employee AML training records	Duration of employment + 5 years	HR system + compliance archive
Internal investigations and escalations	10 years	Secure archive, legal privilege when applicable

🔒 All AML records are stored in encrypted systems with restricted access. Records are available for inspection by competent authorities (UIAF, DIAN, FinCEN, CBUAE) upon lawful request. No records are destroyed before the expiry of the applicable retention period.

08 AML TRAINING

Staff awareness and competence

Training Program	Frequency	Audience	Format
AML Fundamentals (FATF, SARLAFT, BSA, UAE AML Law)	Annual mandatory + onboarding	All staff and contractors	E-learning + written test (min. 80% pass score)
Red Flags & Suspicious Activity Recognition	Annual	Operations, KYC, customer-facing teams	Case studies + scenario workshop
Sanctions Compliance & OFAC screening	Annual	All staff	E-learning
MLRO Role & Internal Reporting Procedures	Annual + upon MLRO appointment	MLRO, Compliance Officer, Management	In-person training + certification
Customer-Facing AML Communication	Annual	Customer support, sales, broker management	Role-play scenarios

Training completion records are maintained by the Compliance Officer and reviewed by senior management annually. Failure to complete mandatory training may result in disciplinary action.

09 COMPLIANCE OFFICER / MLRO

Roles and responsibilities

9.1 Money Laundering Reporting Officer (MLRO)

Sentu designates a Money Laundering Reporting Officer (MLRO) for each regulated jurisdiction. The MLRO is responsible for:

- Receiving and evaluating internal suspicious activity reports from employees.
- Making the determination to file or not file a SAR/STR/ROS with the relevant authority.
- Maintaining all AML records and ensuring regulatory compliance.
- Reporting directly to senior management and/or the Board on AML matters.
- Keeping abreast of regulatory developments and updating the AML program accordingly.
- Conducting or overseeing the annual AML risk assessment.

9.2 Independence and Non-Retaliation

The MLRO has independence in the exercise of their functions and direct access to senior management. Sentu prohibits any form of retaliation against employees who, in good faith, report suspicious activity or raise AML concerns. Any retaliation will result in immediate disciplinary action.

9.3 Contact

AML/Compliance inquiries and internal suspicious activity reports should be directed to: fa.acosta@legalnova.co (confidential channel). This email is monitored exclusively by the MLRO and senior management.

10 AUDIT & REVIEW

Governance of this policy

Review Activity	Frequency	Responsibility
Annual AML Risk Assessment	Annually (January)	MLRO + External AML Advisor
AML Policy Review and Update	Annually or when regulatory changes require it	MLRO + Legal + Senior Management approval
Internal AML Audit	Annually	Internal Audit function or appointed external auditor
Independent External AML Review	Every 2 years or upon regulatory request	External specialized AML firm
Regulatory Examination Preparation	Ad hoc (prior to any scheduled examination)	MLRO + Legal + Finance

📋 This AML Policy is approved by Senior Management and constitutes a binding commitment of Sentu Services and all its affiliated entities. Non-compliance with this policy may result in disciplinary measures, termination of the relationship, and referral to regulatory authorities.

Policy Version: 1.0 | Effective Date: March 10, 2026 | Next Review: March 2027

Approved by: Senior Management — Sentu Services Group

Questions: fa.acosta@legalnova.co | sentuservices.com/aml-policy