

NIVALIS

**KYC & AML COMPLIANCE MANUAL NIVALIS DIGITAL SERVICES LLC Incorporated in
Nevis Effective date: May 22, 2025 with registered company number: L23715**

INDEX

1. BUSINESS IDENTIFICATION AND GENERAL DESCRIPTION
2. INTERNATIONAL AND NATIONAL REGULATORY FRAMEWORK
3. CONCEPT OF MONEY LAUNDERING AND TERRORISM FINANCING
4. ORGANIZATIONAL STRUCTURE AND INTERNAL POLICIES

5. Customer Due Diligence (CDD) and Know Your Customer (KYC)
6. CUSTOMER ACCEPTANCE POLICY
7. Enhanced Due Diligence (EDD)
8. TRANSACTION MONITORING AND REPORTING
9. IDENTIFICATION AND REPORTING OF SUSPICIOUS TRANSACTIONS
10. HIGH-RISK JURISDICTIONS AND SANCTIONED ENTITIES
11. RECORD KEEPING AND DATA PROTECTION
12. INTERNAL CONTROL BODIES AND FUNCTIONS
13. STAFF TRAINING AND AWARENESS
14. INDEPENDENT REVIEW AND AUDITOR
15. ANNEXES

1. IDENTIFICATION AND GENERAL DESCRIPTION OF THE BUSINESS

1.1. Legal Name and Registered Address

- **Company Name** : NIVALIS DIGITAL SERVICES LLC
- **Jurisdiction** : Nevis
- **Entity Type**: Limited Liability Company (LLC)
- **Registered Address**: Hermitage, St John 's Parish, Nevis.
- **Date of Incorporation** : May 22, 2025
- **Commercial Registration Number** : L23715

1.2. Nature and Scope of Activities

NIVALIS DIGITAL SERVICES LLC is dedicated to the private facilitation of purchase and sale transactions of digital assets (cryptocurrencies and other digital tokens) between pre-verified and authorized counterparties, primarily corporate and institutional clients.

The company does not provide **public exchange services** or act as **an intermediary between retail users**. **NIVALIS operates under a bilateral** transaction model with an exclusive focus on **digital asset exchanges in significant volumes** , commonly referred to as **blocks** .

Key services:

- Facilitation of buying/selling digital assets between institutional parties.
- Structuring of OTC transactions under specific contractual conditions .
- Technical and administrative support for transfers and verification of funds.

NIVALIS DIGITAL SERVICES LLC does not offer:

- Open access to markets or trading platforms.
- Cryptocurrency custody services.
- “retail exchange ” type processing .
- Services to users without verified identification or documentary proof of origin of funds.

1.3. Regulatory Framework and Compliance Policy

Currently, the jurisdiction of Nevis does not have a specific legislative framework for licensing cryptoasset or digital asset operations. However, NIVALIS DIGITAL SERVICES LLC has opted to adopt a **voluntary and rigorous compliance framework** inspired by the international standards of the following entities:

- **Action Task Force (FATF)**
- **European Union AML Directives 5 and 6**
- **FinCEN (US) and OFAC (sanctions) guidelines**
- **MONEYVAL and CARICOM Recommendations**

This decision to align with international best practices seeks not only to mitigate operational and reputational risks, but also to ensure that financial institutions and banking counterparties can validate NIVALIS's compliance framework as equivalent to an international standard .

1.4. Target Customers and Market Segmentation

NIVALIS DIGITAL SERVICES LLC's business model deliberately excludes the general public . It is geared toward institutional clients, professional investors, and corporate entities with structured transactions and valid legal documentation .

Accepted customer segments include:

- OTC (Over-the-Counter) trading desks
- Investment funds , family offices and trust entities

- Financial institutions with exposure to crypto assets
- Multinational companies with diversified digital treasury
- High-net-worth individuals through legal vehicles (trusts, holdings, private foundations)

1.5. Estimated Trading Volume and Thresholds

The typical operation managed by NIVALIS DIGITAL SERVICES LLC contemplates an estimated minimum volume of USD 25,000 per transaction , with regular flows that can reach ranges above USD 500,000 in blocks .

minimum operating threshold is established in order to:

- Ensure the ability to verify the origin of funds.
- Avoid unnecessary exposure to retail transaction risk.
- audit resources .

1.6. Commitment to Transparency and Traceability

As part of its general governance policy, NIVALIS DIGITAL SERVICES LLC ensures that :

- clients or those without a clear legal structure will not be allowed to operate.
- Every operation will be traceable from its beginning to its execution .
- The company will maintain complete records of KYC documentation, financial justification , and internal reviews, as stipulated in this manual.

2. INTERNATIONAL AND NATIONAL REGULATORY FRAMEWORK

2.1. Regulatory Context in Nevis

The Nevis jurisdiction, through the Financial Services **Regulatory Commission (FSRC)** , provides a legal framework for the formation of corporate entities, as well as for traditional financial services such as banking, insurance, or trust funds. However, **there is currently no legislation or specific license issued by the FSRC for activities related exclusively to the purchase and sale of digital assets** , provided that one does not act as a financial intermediary open to the public .

NIVALIS DIGITAL SERVICES LLC does not operate as a cryptocurrency broker, exchange, or custodian , and does not offer services to Nevis or global retail users. Its business model is limited to the **direct purchase of crypto assets from institutional liquidity providers and wholesale sales to pre-vetted institutional clients** .

Therefore, and in accordance with the current interpretation of the legal framework in Nevis:

- **No local license is required or issued for these operations .**
- There is no handling of third-party funds.
- No public capital raising is carried out .
- No open market exchange or custody services are offered on behalf of clients.
- The transactions are bilateral and contractually structured between verified parties.

2.2. Voluntary Commitment to Compliance

In the absence of specific regulations , the company has implemented a self- regulation system aimed at ensuring the traceability, legality, and transparency of its operations. This framework includes internal policies aligned with the following international standards :

- The **40 Recommendations of the FATF .**
- **The European Union directives** AMLD5 and AMLD6 .
- **OFAC** regulations , UK and UN sanctions **lists** .
- The guidelines issued by **FinCEN (USA)** .
- The principles suggested by **MONEYVAL** and the standards of the **Caribbean Cooperation Forum (CARICOM)** .

This compliance commitment aims to:

- Facilitate relationships with international correspondent banks and custodians.
- Mitigate legal and reputational risk.
- Promote confidence in the structure and transparency of the operation .
- Comply with indirect regulatory requirements in countries where their institutional counterparts reside.

2.3. Internal Supervision and Controls

Although the FSRC does not impose direct oversight over this activity, **NIVALIS DIGITAL SERVICES LLC has developed a robust governance structure** , which includes:

- **Formal appointment of a Compliance Officer** with operational independence.
- Establishment of a risk committee that evaluates each operation and each client.
- **Periodic internal audits on AML / KYC policies** .
- Mechanisms for documenting , reviewing and storing sensitive information for at least 5 years .

- Adoption of technological controls for the detection of atypical transactions .

3. CONCEPT OF MONEY LAUNDERING AND FINANCING OF TERRORISM

3.1. Definition of Money Laundering (ML)

Money laundering is the process of creating a legitimacy appearance for illicitly obtained funds or assets . This process is generally carried out through a sequence of operations designed to conceal the origin, nature, location , ownership, or control of said funds.

most common stages of money laundering are:

1. **Placement** : Introduction of illicit funds into the financial system (e.g., deposits , purchase of **digital** assets, etc.).
2. **Layering** : Separation of funds from their original source through multiple transactions (sending between wallets, converting between **cryptocurrencies** , using mixers, etc.).
3. **Integration** : Reintroduction of funds into the economic system as apparently legitimate (e.g., acquisition of **goods** , legal investments, corporate transactions).

3.2. Definition of Terrorist Financing (TF)

Terrorist financing involves the provision or collection of funds with the knowledge, intent , or suspicion that these funds will be used , in whole or in part, to support terrorist acts, individuals, or organizations with terrorist aims. What distinguishes FT is that the funds may have **legal or illegal** origins , which presents an additional challenge in its detection and monitoring.

In the context of cryptoassets, common mechanisms used for terrorist financing include:

- or split transfers between wallets.
- Donations via cryptocurrency to extremist entities.
- verification measures .

3.3. Specific Risks in the Digital Asset Environment

Digital assets, due to their technical design and growing adoption , represent an opportunity for illicit actors seeking to evade traditional controls. The characteristics of these assets that increase AML/CFT risk include:

- **Decentralization : Absence** of regulated intermediaries.
- **Partial transparency**: Visibility in the blockchain, but anonymity in the identity of the actual holder.
- **High liquidity and speed**: Allows the transfer of large amounts of money in minutes, across multiple jurisdictions .

- **technological innovations** : New protocols, tokens, networks and services appear frequently without supervision .

In particular, the use of **privacy-focused coins** (such as Monero, Zcash, or Dash), **mixing services** (mixers/tumblers), and the use of multi - **signature wallets or wallets in unmonitored jurisdictions represent** critical risk factors .

3.4. NIVALIS DIGITAL SERVICES LLC's Commitment to Risk Mitigation

NIVALIS DIGITAL SERVICES LLC adopts a proactive, preventative, and dynamic approach to the threats of money laundering and terrorist financing. Measures taken include, but are not limited to:

- Enhanced identity verification (KYC) for all customers before starting operations.
- Comprehensive review of the transactional profile and continuous monitoring of deviations.
- Assessment of corporate relationships and structures to identify ultimate beneficial owners (UBOs).
- Automatic and periodic verification against international sanctions lists (OFAC, UN , EU , UK).
- Application of the “know your trade ” (KYT) principle to detect suspicious behavior even within already verified accounts.
- annual review and update of the ML/FT risk matrix, including analysis by country , client type, volume and asset type.

3.5. Institutional Objective

The core objective of NIVALIS DIGITAL SERVICES LLC is to ensure that its infrastructure, personnel, channels, and operations **are not used directly or indirectly** for money laundering or terrorist financing. This is achieved not only through technological and operational controls , but also through a cross - functional compliance culture, ongoing training, and effective cooperation with banking , legal, and technological counterparties .

All actions are aimed at preserving the integrity of the global financial system, protecting the company's reputation, and providing confidence to its institutional clients and suppliers .

4. ORGANIZATIONAL STRUCTURE AND INTERNAL POLICIES

4.1 Introduction

The organizational structure of NIVALIS DIGITAL SERVICES LLC has been designed to ensure the proper implementation , monitoring, and compliance with international and local regulations on the prevention of money laundering and terrorist financing (AML), as well as to ensure that internal policies related to KYC (Know Your Customer) and due diligence are executed efficiently and effectively. This structure facilitates the clear assignment of responsibilities and powers,

encourages appropriate supervision and control, and promotes an organizational culture focused on compliance, ethics , and transparency.

4.2 Organization and Key Roles

4.2.1 Board of Directors

The Board of Directors is the highest supervisory and governance body within NIVALIS DIGITAL SERVICES LLC and has the following AML/KYC responsibilities:

- Approve and periodically review policies and procedures related to the prevention of money laundering and terrorist financing.
- Allocate the necessary resources to ensure the effective implementation of these policies .
- Ensure that the Compliance Officer has sufficient independence and authority to carry out his or her duties.
- audit and risk reports related to AML/KYC, and take necessary steps to mitigate any findings.

4.2.2 Compliance Officer

The Compliance Officer is directly responsible for managing and enforcing the company's AML/KYC policy. His or her main duties include :

- Implement and update AML/KYC policies and procedures, ensuring they are aligned with current Nevis legislation and international standards .
- Coordinate and supervise due diligence processes, monitoring operations, and reporting suspicious activities.
- Maintain effective communication and coordination with regulatory authorities and other relevant bodies.
- Conduct periodic risk assessments and prepare reports for the Board of Directors.
- Promote and coordinate AML/KYC training and awareness for all staff.
- Ensure the confidentiality of information handled in compliance processes.

4.2.3 Compliance Team

The compliance team, under the supervision of the Compliance Officer, plays a key role in the practical execution of AML / KYC controls, with responsibilities such as:

- Conduct internal reviews and audits to verify the correct application of policies .
- Manage and document due diligence of clients and related third parties.

- Support in the identification and analysis of unusual or suspicious operations.
- Maintain up-to-date customer records, operations, and compliance reports.

4.2.4 Operational and Administrative Staff

All NIVALIS DIGITAL SERVICES LLC staff, including operational, administrative, and customer service areas, must :

- Strictly comply with the procedures and controls established in the AML/KYC policies .
- Be alert to detect any unusual operations , conduct, or behavior that may pose a risk of money laundering or terrorist financing.
- or unusual activity or transaction to the Compliance Officer .
- Actively participate in training and refresher courses related to money laundering prevention .

4.3 Fundamental Internal Policies

4.3.1 Legal and Regulatory Compliance

NIVALIS DIGITAL SERVICES LLC is committed to operating in strict compliance with all applicable laws and regulations in Nevis regarding the prevention of money laundering and terrorist financing. This includes complying with the requirements established by national agencies, as well as adopting internationally recommended best practices , to protect the integrity of the company and the global financial system.

4.3.2 Ethics and Transparency

The company promotes an organizational culture based on ethics , responsibility, and transparency, where all business activities are conducted in accordance with sound legal and moral principles . All employees are expected to act with integrity, report any anomalies , and maintain a constant commitment to preventing illicit activities .

4.3.3 Confidentiality and Data Protection

NIVALIS DIGITAL SERVICES LLC guarantees the protection and confidentiality of all personal, financial, and business information of its clients, employees, and third parties involved, in compliance with applicable data protection laws in Nevis and international standards . Access to information is strictly limited to authorized personnel, and technical and organizational measures are implemented to prevent unauthorized access or improper disclosure.

4.3.4 Risk Identification and Management

The company adopts a risk-based approach to preventing money laundering, which involves:

- Identify and assess the risks inherent to your services, customers, jurisdictions, and operations.

- Establish controls proportional to the levels of risk detected, increasing due diligence in cases of higher risk.
- Periodically review the risk assessment to adapt to changes in the regulatory or business environment.

4.3.5 Continuous Reporting and Monitoring

Mechanisms are established for the ongoing monitoring of the company's operations and activities, in order to detect atypical or suspicious patterns that may indicate money laundering or terrorist financing. Suspicious activities will be evaluated and, if necessary, reported to regulatory authorities in accordance with established procedures.

4.3.6 Continuing Training

Staff training and awareness is a fundamental pillar for effective compliance with AML/KYC policies . Therefore, periodic training programs are conducted that address :

- Basic and advanced concepts of money laundering and terrorist financing.
- Specific obligations and responsibilities of each position.
- Internal procedures and warning signs for detecting suspicious transactions .
- Regulatory updates and changes in internal policies .

4.4 Independence and Authority of the Compliance Officer

The Compliance Officer enjoys the autonomy to perform his or her duties without undue interference and has the authority to access all information necessary to fulfill his or her responsibilities. He or she may also escalate any risk or noncompliance situation to the Board of Directors without restriction.

4.5 Review and Update of Policies

NIVALIS DIGITAL SERVICES LLC undertakes to regularly review and update its AML/KYC policies and procedures, at least once a year in response to regulatory changes or changes in the company's risk profile, in order to maintain their validity, suitability and effectiveness.

4.6 Documentation and Registration

All actions, decisions, evaluations, and reports related to the prevention of money laundering must be documented and securely archived, facilitating internal audits , regulatory reviews, and ensuring the traceability of operations.

5. Customer Due Diligence (CDD) and Know Your Customer (KYC)

5.1 Introduction

NIVALIS DIGITAL SERVICES LLC, a company duly incorporated under the laws of Nevis, understands that although **it is not required to obtain a financial license as a virtual asset service provider (VASP)**, because **it does not act as a broker, exchange or custodian of cryptocurrencies**, **it is subject to compliance with the basic principles and obligations of prevention of money laundering (AML) and financing of terrorism (CFT)**, according to the legal framework in force in Nevis.

Pursuant thereto, and as part of a corporate policy of responsible compliance, NIVALIS DIGITAL SERVICES LLC has **proactively implemented a robust compliance program**, including formal Customer Due Diligence (CDD) and Know Your Customer (KYC) policies, which follow international standards such as those set forth by the Financial Action Task Force (FATF), in addition to local requirements in Nevis contained in the **Anti-Money Laundering Regulations** and the **Proceeds of Crime Act**.

This section clearly establishes the measures adopted by the company to adequately identify, verify, and monitor its clients, despite not being required to be licensed because it does not engage in financial intermediation activities or manage third-party funds.

5.2 Commitment to Local and International Compliance

Although the nature of NIVALIS DIGITAL SERVICES LLC's operations does not require a financial license under the Nevis regulatory framework, the company **recognizes that the effective implementation of KYC/AML processes is mandatory** for any business entity that maintains business relationships with counterparties and clients, both local and international.

The company adopts and reinforces these policies as part of its commitment to:

- Prevention of being used as a vehicle for illegal operations.
- The transparency and traceability of its operations.
- Cooperation with tax, financial and police authorities if necessary.
- Building trust with banking correspondents and global partners.

5.3 Scope of CDD and KYC Policies

These policies apply to **all clients** — natural or legal persons — with whom NIVALIS DIGITAL SERVICES LLC maintains or intends to maintain a business relationship, including final beneficiaries and related third parties.

The company refrains from establishing relationships with individuals or entities that cannot be identified with certainty, or whose risk profile exceeds the acceptable threshold in accordance with its risk matrix.

5.4 General Identification and Verification Procedures

5.4.1 Natural Persons

Minimum requirements include:

- photo ID (passport or national ID) .
- Proof of address issued within the last three months.
- Valid contact information .
- Verification of the source of funds, as appropriate .
- Declaration as to whether the client is a Politically Exposed Person (PEP).

5.4.2 Legal Entities

Required:

- Certificate of incorporation .
- Articles of association or operating agreement.
- Identification of legal representatives and directors .
- Identification of all final beneficiaries with a stake exceeding 25%.
- Documents that support the legitimacy and origin of the funds that will be used in the business relationship .

All documents are subject to manual validation and/or validation by reliable automated systems, with additional support from public or private sources , depending on the risk.

5.5 Ultimate Beneficiary and Actual Controller

NIVALIS DIGITAL SERVICES LLC considers it vitally important to accurately identify the ultimate beneficiary, even when the client's legal structure partially obscures it. Transparency criteria aligned with international recommendations are applied, considering the ultimate beneficiary to be the person(s) who:

- Directly or indirectly own more than 25% of the shares or control the entity.
- Have the power to decide or not control by other means.

5.6 Client Risk Assessment

Each client is evaluated based on a risk matrix that considers:

- Economic activity and nature of the business.
- Jurisdiction of residence and operation .
- Expected trading volume.
- Use of complex structures.

- Public exhibition or background .

Based on this assessment , clients are classified as low, medium, or high risk, and due diligence levels are adjusted accordingly.

5.7 High Risk Clients

In the case of high-risk clients, **Enhanced Due Diligence (EDD) measures are applied** , such as additional interviews, obtaining extended documentation and more frequent review of the transactional profile, in accordance with point 7 of this Manual.

5.8 Documentation and Conservation

All documentation obtained during the identification and verification process is securely stored in accordance with the principles of confidentiality and data protection . Records are retained for a minimum of five (5) years , even after the business relationship has ended, in compliance with current legislation .

5.9 Operational Limitations and Non-Financial Nature

NIVALIS DIGITAL SERVICES LLC expressly declares that:

- It does not carry out brokerage, exchange, or cryptocurrency trading activities.
- Does not offer custody or virtual asset management services.
- It does not mediate or hold third-party funds in any currency, fiat or digital.
- It does not perform regulated services as a financial institution under the laws of Nevis.

Therefore, it is not subject to the licensing regime for financial services providers, although it **is aligned with the preventive KYC/AML obligations** established by legislation for all entities operating professionally.

6. CUSTOMER ACCEPTANCE POLICY

6.1 General Principles

NIVALIS DIGITAL SERVICES LLC has adopted a **Client Acceptance Policy (CAP)** that is clear, prudent, and proportionate to the type of services it offers. Although it does not act as a financial services provider or is subject to licensing by the Nevis authorities, the company recognizes that its continued existence and reputation **as a** legally constituted entity requires appropriate standards in the selection and maintenance of business relationships.

This policy is implemented to ensure that:

- Only clients whose identity, activity and source of funds are verifiable and legitimate will be admitted .

- Do not establish relationships with people or entities linked to illicit activities or with high, non-mitigable risks.
- The company is not used — inadvertently or intentionally — as an instrument for money laundering, terrorist financing, tax fraud, evasion , financial crimes or complex schemes without economic justification .

Customer Acceptance Criteria

Acceptance of clients is subject to **prior evaluation** , and only those who meet the following minimum criteria **will** be admitted :

a) Verifiable identity

The identity of the client, including its final beneficiaries and legal representatives, must be **complete, consistent, current, and verifiable** through official documentation and /or reliable sources.

b) Legitimate and verifiable activity

legal, ethically acceptable economic activities , preferably documented in public records , contracts, websites , or verifiable business references.

c) Clear and justified source of funds

Every client must provide credible and sufficient information about the origin of the funds and resources that they will eventually transact or link to their operations with the company.

d) Compatible jurisdictions

Access is restricted to individuals or companies domiciled or operating in **sanctioned jurisdictions, jurisdictions with international restrictions, or those listed as high risk by the FATF** . Clients residing or incorporated in countries under broad economic sanctions are not accepted .

e) Legitimate purpose

The reason why the client wishes to establish a business relationship with NIVALIS DIGITAL SERVICES LLC must have a **legitimate , coherent and aligned basis with the non-financial services that the company effectively provides** .

f) Transparency of corporate structure

When the client is a legal entity , it must disclose its entire structure, including intermediaries, holding companies or foundations, as well as the final beneficiaries with 25% or more of non - controlling interest .

g) No connection with prohibited activities

Clients who have not been related to:

- Fraudulent activities, pyramid schemes or opaque investment schemes.
- Sale or promotion of unregulated or fraudulent financial products.
- Money laundering, terrorism, drug trafficking , human trafficking or public corruption .
- Unregulated digital asset service providers acting as custodians, exchanges or brokers.

6.3 Unsupported Customer Segments

As a precaution , **the company has defined certain customer profiles that will be automatically rejected , except** in exceptional cases, documented and approved by Senior Management . These include:

- Individuals or entities subject to international sanctions (UN, OFAC, EU).
- Politically Exposed Persons (PEP) without solid economic justification .
- Clients who refuse to provide KYC information or supporting documents.
- Companies without clear operations, without digital presence or commercial traceability.
- Natural persons acting as "front men" with no apparent relationship to the declared activity .
- Legal entities incorporated in high-risk jurisdictions without economic justification .
- Clients whose business model requires a financial or virtual asset license to operate legally, if they do not already possess one.

6.4 Risk Assessment before Acceptance

All clients undergo a **risk assessment prior to the start of the relationship , in which** variables such as:

- Jurisdiction of origin .
- Type of activity and economic sector .
- Expected transactional volume.
- Complexity of the structure.
- Compliance history.
- Public exhibition or background .

Only clients classified as **low or acceptable medium risk** are considered eligible. High-risk clients require special approval and additional measures (see Section 7 – Enhanced Due Diligence).

6.5 Acceptance Procedure

client admission process follows these stages :

1. **Reception of preliminary application with** admission form .
2. **Document review by the** Compliance Officer.
3. **Initial risk assessment and** validation of restrictive lists.
4. **- checking of data using** public sources or third parties.
5. **Final approval by Senior** Management .
6. **Secure archiving of** electronic documents and records .

Without completing these steps, **client activation and the start of any commercial activity is not permitted** .

6.6 Periodic Review of Clients

All accepted clients will be subject to a **periodic review** , **based** on their risk level, to verify whether their profile, structure, jurisdiction , or activity has changed. This ensures that the initial acceptance **remains** valid based on current criteria.

7. ENHANCED DUE DILIGENCE (EDD)

7.1 Definition and Approach

Enhanced Due Diligence (EDD) is a set of additional procedures that NIVALIS DIGITAL SERVICES LLC proactively applies to clients or situations that present a higher risk of money laundering, terrorist financing or financial abuse .

Although the company does not engage in activities that require a financial license under Nevis law, it implements these measures voluntarily as part of its commitment to the principles of transparency, operational integrity, and alignment with international standards such as those of the FATF.

7.2 Objective

The objective of the EDD is:

- a deeper understanding of the nature of certain business relationships.
- Further validate the legitimacy of the source of funds.
- Ensure that the relationship with the client does not represent a reputational or compliance risk.

7.3 Criteria for Applying EDD

The EDD is activated in the following scenarios, among others:

- Clients operating from **high-risk jurisdictions** , according to FATF or similar bodies.
- Politically Exposed Persons (PEP), family members or close associates.
- Clients whose **corporate structure is particularly complex or opaque** .
- Operations that, due to their nature or volume, **do not align with the declared profile** .
- Clients who **cannot provide verifiable documentation of their economic activity or source** of funds.
- **inconsistencies** are detected between the data provided and independent verification .
- Clients with sensitive activities or international exposure .

7.4 Measures Applicable under EDD

In cases requiring EDD, one or more of the following measures are applied, depending on the level of risk:

a) Collection of additional information

- Financial statements, contracts, tax returns, or evidence of income.
- Detailed evidence of the source of funds.
- Documentation demonstrating the legitimacy of the operations .

b) Intensified verification

- Confirmation of identity and documents by independent means or official sources.
- Verification of the final beneficiary through public records or external KYC services.
- Validation of commercial or reputational references.

c) Approval of Senior Management

Any relationship with high-risk or EDD-subject clients will require direct **approval from Senior Management prior to** the commencement of any business activity.

d) Continuous monitoring

- More frequent monitoring of transactions or interactions.
- Periodic evaluation of behavior and policy compliance .
- Request for more frequent document updates.

e) Rejection or termination of the relationship

If EDD requirements cannot be met or if the risk cannot be adequately mitigated, the company **reserves the right to reject or terminate** the business relationship immediately and without prejudice.

7.5 Justification of the Policy

current legislation in Nevis does not require NIVALIS DIGITAL SERVICES LLC to implement AML/KYC compliance policies comparable to a licensed financial institution or digital asset service provider, the company:

- **Recognizes its corporate responsibility** to the international community.
- **You want to avoid being used** as a vehicle for opaque structures or illicit purposes .
- **Act proactively to** ensure sustainability, credibility, and acceptance by correspondent banks, business partners, and global counterparties.

This position allows the company **to prevent reputational risk, protect its legal environment and facilitate its access to legitimate services** , including financial services, despite operating within a non-compulsory license regime .

8. MONITORING AND REPORTING OF TRANSACTIONS

8.1 Commitment to International Good Practices

Although NIVALIS DIGITAL SERVICES LLC is not required by Nevis law to comply with regulatory requirements of financial institutions or licensed virtual asset service providers, the company has **voluntarily adopted a transaction control and monitoring framework** to ensure a safe, transparent and internationally compliant trading environment .

Transaction monitoring is a key tool in detecting unusual transactions or transactions potentially linked to illicit activities , and is an essential part of the company's commitment to AML/KYC policies .

8.2 Scope of Monitoring

NIVALIS DIGITAL SERVICES LLC applies a policy of periodic review and analysis of transactions under the following criteria:

- **Consistency with the client's profile:** Transactions must correspond to the economic and operational profile declared by the client.
- **Unusual volume or frequency:** Transactions that, due to their size , frequency or nature, deviate significantly from the client 's historical pattern are reviewed .
- **Sensitive jurisdictions: Special** attention is paid to operations related to countries included in high-risk lists by organizations such as the FATF or OFAC.

- **Unusual payment methods: Transactions** that use opaque mechanisms, complex structures, or unusual financial instruments will be **subject** to additional review .

8.3 Tools and Procedures

a) Periodic manual review

The compliance team regularly reviews customer transactions, including income, expenses, invoicing , and supporting documentation , if applicable. Any deviation from expected behavior generates an internal alert for further evaluation .

Risk classification systems

Proprietary risk matrices are used to assign a risk level to each client. These matrices consider factors such as:

- Nationality and residence
- Declared economic activity
- Legal structure
- Operating history with the company
- Jurisdictions involved

c) Internal alert registry

Any transaction that raises concerns is documented in an **Internal Alert Log** , which is managed confidentially by the Compliance Officer, who determines whether corrective action or further investigation is appropriate .

Internal Reporting and Evaluation

While NIVALIS DIGITAL SERVICES LLC is not subject to a mandatory reporting entity such as a national Financial Intelligence Unit (FIU), it has established the following practices :

- **Internal escalation:** Every suspicious transaction is evaluated by the Compliance Officer and, if appropriate, reported to Senior Management for analysis .
- **Review of additional documentation:** If necessary, the client may be asked for additional information **to** validate the origin and destination of the funds.
- **Temporary suspension of the business relationship :** If there is a well-founded doubt about the legitimacy of the transaction and the risk cannot be mitigated, the company reserves the right to suspend or close the customer's account as a precautionary measure.

8.5 Commitment to Transparency

NIVALIS DIGITAL SERVICES LLC expressly declares that **it does not facilitate, mediate, or participate in the execution of operations with crypto assets under custody, broker or exchange schemes** , and that all its activities are strictly of a corporate, administrative and advisory nature .

However, in line with its **enhanced compliance policy and business ethics** , the company:

- Internally documents the operations carried out by its clients within its administrative platforms.
- Maintains mechanisms for verifying the origin of funds and operational consistency.
- It remains willing to collaborate, if required, with authorities or banking entities in the verification of information , always within the applicable legal framework.

Shall we now move on to **Point 9: Identifying and Reporting Suspicious Operations ? This point is key to closing the** operational block of monitoring.

You said:

more extensive if you can, double the information and texts

ChatGPT said:

Of course. Below I present **Point 8: Transaction Monitoring and Reporting** with an **expanded version** , specifically adapted to the operational reality of **NIVALIS DIGITAL SERVICES LLC** , incorporated in Nevis and not subject to mandatory financial licensing. The wording seeks to demonstrate to the bank or other third parties that the company adopts **solid , reasonable, and proportionate voluntary measures** , in line with international standards .

8. MONITORING AND REPORTING OF TRANSACTIONS

8.1 General Approach

NIVALIS DIGITAL SERVICES LLC, although not subject to the regulatory licensing requirements applicable to financial institutions, virtual asset service providers or exchange platforms under Nevis law, voluntarily adopts policies of proactive and **constant monitoring of transactions carried out by its clients** .

This approach not only prevents its misuse by third parties for illicit purposes (such as money laundering or terrorist financing), but also strengthens your business reputation , allows for better traceability of your commercial activity, and facilitates trusting relationships with banks and other international suppliers.

The company does not offer exchange, **intermediation , trading, custody, or brokerage services for crypto assets** , but recognizes that any corporate structure can be vulnerable to misuse if a system for monitoring and evaluating transactional behavior is not implemented .

8.2 Guiding Principles

NIVALIS DIGITAL SERVICES LLC monitoring policies are based on the following principles :

- **Risk proportionality:** Activities are monitored according to the risk profile assigned to each client.
- **Early prevention :** The goal is to identify and act on warning signs before irregular behavior materializes.
- **Economic coherence :** All operations must be logically related to the client 's activity, volume and jurisdiction .
- **Documented transparency:** Each review or non-alert is recorded in an orderly, traceable and accessible manner.
- **Institutional responsibility:** Decisions are made under a structured criterion, with participation of the Compliance Officer and validation by Senior Management when necessary.

8.3 Monitoring Mechanisms

a) Periodic review of operations

The Compliance Officer conducts periodic reviews of transactions reported by clients, whether through internal systems, administrative platforms, or other pre-authorized channels. These reviews focus on:

- Amounts, frequency and nature of operations.
- Comparison with the customer 's historical behavior.
- Consistency with the declared economic , geographic and legal profile .

Alert generation criteria

The company has developed an **internal risk matrix** with warning indicators, including:

- Receiving or sending funds from jurisdictions classified as non -cooperative or high risk (according to FATF, OFAC or EU).
- operating patterns without apparent justification .
- Opaque corporate structures, difficult to trace, or with the presence of non-transparent trustees.

- Use of unconventional payment methods or platforms that are difficult to verify .
- Suspicious interactions with third parties not linked to the contractual purpose declared by the client.

8.4 Documentation and Traceability

record retention protocols. This includes :

- Electronic transaction records .
- Captures or backups of transfers, invoices or attached contracts.
- Compliance Officer review log, with date , observations and evaluation results .
- Decisions made, including corrective actions, requests for clarification from the client, or escalation to Senior Management .

the company to demonstrate that it acts with diligence, transparency and responsibility in the event of a request from correspondent banking entities or international organizations, despite not being legally required to report to a Financial Intelligence Unit in Nevis.

8.5 Procedure for Unusual or Suspicious Operations

a) Initial investigation

operation outside the expected pattern is detected , the Compliance Officer requests additional documentation from the client, which may include:

- Written statement of the purpose of the transaction .
- Bank receipts for the origin or destination of the funds.
- Identification of third parties involved in the operation .

b) Risk assessment and decision

Based on the information received , the Compliance Officer assesses whether:

- The transaction is justifiable **and consistent** with the customer's profile, in which case it is filed as closed.
- The operation presents unmitigated **risks** , which requires the case to be raised to Senior Management to decide on the continuity of the relationship .
- The transaction constitutes an **improper use of the corporate structure** , in which case the contractual relationship is terminated and, if appropriate, external legal advisors or entities with which the company maintains business relationships are informed.

8.6 Cooperation with Banks and Third Parties

Although Nevis law does not impose a formal reporting obligation on NIVALIS DIGITAL SERVICES LLC to state agencies, the company undertakes to:

- **Cooperate in good faith** with banks and international entities that require verification of information about customers or transactions, always respecting applicable data protection legislation .
- Provide **internal reports certified** by the Compliance Officer in cases where a financial institution requests evidence of internal control.
- Act as an active part in **preventing the abusive use of the company for illegal purposes** .

8.7 Conclusion

NIVALIS DIGITAL SERVICES LLC, while not performing the functions of a licensed financial services provider, applies serious and systematic controls in its relationships with clients and in the monitoring of operations carried out through its administrative infrastructure.

This policy is not an imposed obligation , but rather a **voluntary manifestation of its institutional commitment to compliance, transparency and integrity** , which are essential for operating in the international corporate ecosystem with legitimacy and trust.

9. IDENTIFICATION AND REPORTING OF SUSPICIOUS TRANSACTIONS

9.1 Institutional Commitment and Voluntary Proactivity

NIVALIS DIGITAL SERVICES LLC recognizes the importance of adopting international best practices in the prevention of money laundering (AML) and terrorist financing (CFT), even though it is not subject to a specific regulatory license in Nevis as it does not act as a broker, custodian, crypto exchange service provider or financial entity.

The company has voluntarily decided to implement internal policies for the **early identification and proper handling of unusual or suspicious operations** , with the purpose of:

- Protect your business structure from misuse.
- Increase the trust of banks, payment gateways, and strategic partners .
- Demonstrate institutional transparency in the face of potential third-party or independent audit requests.

9.2 Internal Definition of Suspicious Operation

A **suspicious transaction** is defined as any activity, conduct, request, or **pattern** that :

- It does not have a justifiable commercial, economic or legal logic .
- Be inconsistent with the customer's stated profile, activity, or previous transactions.
- Prevents clear identification of the origin of funds, destination of resources or final beneficiary.
- Involve actors, structures, or jurisdictions associated with high risk or international sanctions.
- Suggest evidence of cover-up, concealment, fronting, tax evasion , or other misuse of the company's corporate framework.

9.3 Warning Indicators – Operational Risk Matrix

The Compliance Officer maintains a matrix of **warning signs or indicators** , which are periodically reviewed . These signs do not automatically indicate suspicion, but they do trigger an analysis process :

a) Unusual Behaviors and Requests:

- Applications to establish companies without clear commercial activity.
- Instructions for frequent changes of beneficial ownership without explanation .
- Preference for complex structures that do not provide real economic value .

b) Inadequate Documentation and Identification :

- Delays or refusals in the delivery of documentation .
- Delivery of altered or inconsistent documents.
- Difficulty in justifying the legitimacy of the funds.

c) Client Profile and Activity:

- Unclear statements about business activity.
- Absence of tangible links with the jurisdiction of incorporation .
- Customers who express an intention to evade regulations in their country of residence.

d) Jurisdictions and Risk Actors:

- Intervention of entities located in sanctioned or non-cooperating countries .
- Participation of people linked to sensitive or risky activities (illegal mining , unlicensed gambling, opaque P2P operations, etc.).

Atypical Operations :

- Transfers between entities without apparent reason .
- Multiple companies with the same beneficiary with similar structures.

9.4 Internal Identification and Analysis Process

NIVALIS DIGITAL SERVICES LLC implements a formal process for **the detection , analysis , documentation and evaluation of suspicious transactions** , consisting of the following steps:

a) Initial Detection

Any trained team member can identify an alert situation. This information is immediately transmitted to the Compliance Officer, who classifies the situation as :

- Unusual (requires evaluation) .
- Suspicious (requires action) .
- Not relevant (archivable).

b) Formal Registration

Detected operations are documented in an Internal **Operational Risk Assessment Form (FIERO)** , **which** includes:

- Customer identification .
- Date and details of the operation .
- Observed warning indicators.
- Justification or initial explanation from the client, if any.
- analysis and provisional decision .

c) Request for Additional Information

If the situation cannot be clarified immediately, the Compliance Officer may request:

- Contracts, invoices, accounting records or transaction receipts.
- Detailed information of the final beneficiary.
- Evidence of the economic link between related parties.

The client is professionally informed about the need for this review , without generating unnecessary alarm or alerts, preserving confidentiality.

d) Evaluation and Final Classification

With the information collected , a final classification of the operation is carried out :

- **Justified:** The case is closed and filed.
- **Unusual:** Documented and future monitoring is recommended.
- **Suspicious:** Internal escalation protocol is activated.

9.5 Escalation, Documentation and Corrective Action

operation is confirmed as suspicious, the following steps are followed:

a) Internal Escalation:

- Immediate notification to the General Manager and/or Senior Management .
- Evaluation of reputational, legal or strategic implications .
- Decision on continuation , suspension or closure of business relationship .

b) Corrective Measures:

- Voluntary closure of the customer's account or cancellation of service.
- Inclusion in internal list of unacceptable entities.
- Inform partner institutions (banking, legal, etc.), if applicable.

c) **Confidential** **Records:**
All documentation is stored in a **secure digital repository** , accessible only by authorized personnel. The archive preserves:

- Details of the analysis .
- Decisions made.
- Correspondence with the client.
- legal or external recommendations obtained .

9.6 Voluntary Communication to Third Parties

Although not required by a local FIU, NIVALIS DIGITAL SERVICES LLC may voluntarily **and strategically report** suspicious transactions to:

- Correspondent financial institutions or associated banks.
- Legal partners or fiduciaries involved in the operation .

- Payment platforms with which the company collaborates, provided that privacy and the legal framework of Nevis are respected .

9.7 Protection of the Company and Personnel

To ensure the integrity of the process:

- **Total confidentiality is guaranteed** for the informant or collaborator who detects a warning sign .
- **Any form of retaliation** by the customer or third parties **is prohibited** .
- **contractual clause for immediate termination** is defined in cases of confirmed suspicion.

9.8 Culture of Prevention and Continuous Improvement

Detecting suspicious transactions is not a one-time action, but rather part of a culture **of compliance** . Therefore:

- Staff are continuously trained in signal recognition .
- Policies are reviewed every 6 months or when the regulatory environment warrants it.
- Accurate documentation is encouraged , without assuming or prejudging intentions, but without ignoring warning signs .

10. HIGH-RISK JURISDICTIONS AND SANCTIONED ENTITIES

NIVALIS DIGITAL SERVICES LLC, incorporated under the laws of Nevis, understands that geographic risk and international compliance are fundamental components of any effective Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) system . Although our activity **does not require a local financial license nor does it qualify as a cryptocurrency broker or custodian** , we proactively take a risk-based approach and corporate responsibility, implementing strict voluntary controls aimed at ensuring legitimate , traceable, and secure operations.

10.1 General Principles of Geographical Exclusion and Sanctions

NIVALIS DIGITAL SERVICES LLC has adopted a clear policy of exclusion from relationships with individuals, entities or legal structures :

- Domiciled, incorporated or controlled in **jurisdictions recognized by international organizations as high risk or non-cooperative** .
- That appear on international lists of **financial sanctions or economic restrictions** .

- That they are exposed or involved in illicit activities , tax evasion , terrorism, corruption , arms or drug trafficking , massive fraud or operations with undeclared cryptocurrencies.

These restrictions seek to protect the company, its partners, and its payment systems from any legal, operational, or reputational risks.

10.2 Voluntarily Applied International Reference Framework

Although there is no local legal requirement for NIVALIS DIGITAL SERVICES LLC to comply with all regulations of multilateral organizations, the company voluntarily adopts the following sources to define the level of geographic or sanction risk of a country or entity:

- **Action Task Force (FATF)** : Lists of jurisdictions under increased supervision and non-cooperating jurisdictions.
- **Agency for Economic Cooperation and Development (OECD)** : List of non-cooperative tax havens .
- **European Union** : List of non-cooperative tax jurisdictions and high - risk AML/CFT countries .
- **OFAC (USA) list** : Especially the SDN (Specially Designated Nationals).
- **United Nations** : Lists of entities and individuals sanctioned by the Security Council.
- **FCA of the United Kingdom and FINCEN of the United States.**
- **Verified private lists** from providers such as World-Check, Refinitiv, ComplyAdvantage, LexisNexis, and Accuity.

These lists are updated internally every time there is an official review , and are part of the screening processes both during onboarding and subsequent monitoring of the client.

10.3 Jurisdiction Assessment by Risk Levels

geopolitical and financial risk scoring tools :

Low Risk Level:

- Countries with solid AML/CFT regulatory systems .
- Active cooperation with multilateral organizations.
- Automatic exchange of tax information .

Medium Risk Level:

- Jurisdictions with gaps in transparency or enforcement , but with clear commitments to improvement.

- Countries under observation by the FATF or the OECD .

High Risk Level:

- Countries listed by the FATF as non-cooperative .
- States sanctioned by OFAC or the UN Security Council.
- Zones of armed conflict or with governments not internationally recognized.
- Countries without cryptocurrency regulations or with permissive regimes without transparency .

10.4 Business Relationship Exclusion Policies

NIVALIS DIGITAL SERVICES LLC **does not establish relationships with individuals or entities :**

- Linked to **Iran , North Korea, Syria, Cuba, South Sudan , Crimea, Donetsk, Luhansk** or any other sanctioned territory.
- They use **VPN services, obfuscation , or anonymity software** to hide their real location .
- That they cannot **document their tax residence in low or medium risk countries** .
- insist on receiving funds in offshore bank accounts without economic justification .

10.5 Enhanced Control over PEPs and Entities Linked to Sanctions

- All transactions involving Politically Exposed Persons (PEPs) or their close relatives and associates are subject to **Enhanced Due Diligence (EDD)** .
- **Criminal records, negative publications and possible ongoing investigations** are reviewed .
- scandals (e.g. Panama Papers, Pandora Papers) are not approved .

Dynamic Lists and Periodic Updates

- All high-risk and sanctions lists are updated within a period of no more than **30 days** or when an extraordinary event occurs that implies a new relevant sanction .
- Internal monitoring systems use **automatic and manual cross - checking tools** .
- Active clients are constantly scanned using batch screening procedures to detect changes in their status.

10.7 Internal Procedure for Possible Coincidences

1. **Detection** : The automated system or compliance team detects a potential match to a sanctions list .
2. **Preventive Blocking** : The process is temporarily frozen (onboarding, transaction or modification) .
3. **Manual Analysis** : Names, partial matches, aliases, secondary passports or **indirect** links are reviewed .
4. **Internal Report** : A detailed report is prepared and sent to the Compliance Officer.
5. **Escalation** : Senior management makes the final decision .
6. **Immediate unlinking if the match** is confirmed.

Staff Training and Awareness

All compliance and onboarding staff have been specifically trained to:

- Detect red flags related to high-risk jurisdictions.
- Properly interpret sanctions lists.
- search engines , sanctions and risk monitoring.

This training is renewed **annually** , or **earlier if** critical updates to international regulations occur .

10.9 Voluntary Reports to Financial Providers

While NIVALIS DIGITAL SERVICES LLC is not required to report to a local financial authority as a broker or exchange, it maintains the **voluntary practice of collaborating with banking, fiduciary or payment providers** to share preventive information :

- Internal reports on high-risk clients or suspicious structures.
- Documented rejection of operations for geographical or sanctioning reasons.
- or non-freezing decisions .

10.10 Transparency and Corporate Responsibility

Our high-risk jurisdictions and sanctions policy not only seeks to comply with good practices , but also :

- Protect the **company's legal and operational reputation** .
- Ensure sustainable banking and contractual relationships with third parties.
- Facilitate access to legitimate and reliable payment systems.
- Demonstrate our real commitment to **preventing the misuse of offshore structures** .

11. RECORD RETENTION AND DATA PROTECTION

NIVALIS DIGITAL SERVICES LLC, as a private entity incorporated in Nevis, and acting in voluntary compliance with international principles and best practices on the prevention of money laundering (AML) and the financing of terrorism (CFT), establishes formal policies for the retention **of documentation and information collected during its due diligence processes (KYC/EDD)** and for the **protection of its clients' personal and corporate data** .

Although the company **is not legally required to maintain specific licenses as a financial or cryptographic services provider** , it adopts and documents a compliance structure aligned with the reference frameworks of the FATF, the OECD and international regulations on data privacy (e.g. GDPR, PIPEDA, CCPA, among others).

11.1 Mandatory and Voluntary Record Keeping

NIVALIS DIGITAL SERVICES LLC securely retains and stores the following records of its customers and their transactions:

a) Customer Identification Documentation (KYC)

- Copies of your identity document, passport or equivalent.
- Proof of residence (bills, bank statements, address registrations).
- Verification of economic activity or nature of the business.
- Risk profile forms and source of funds statements.

b) Risk Assessments and Classification Matrices

- Initial profiling matrix and periodic re- evaluations .
- Log of alerts or network flags applied.

c) Transaction History

- Records related to payments or transfers received.
- Economic justifications for operations, where applicable.

d) Communications Records

- Emails , forms , and records of customer interaction with compliance .
- Internal logs of analysis or decisions of the Compliance Officer.

11.2 Documentation Retention Period

In accordance with international best practices :

- All records are retained **for a minimum period of five (5) years from :**
 - The **date of termination of the business relationship** .
 - The **last transaction carried out** , if there is no **formal contractual** relationship .
- In cases of suspicious transactions or ongoing investigations, documentation is retained for the period required by the competent authority or until the internal review process is completed .

11.3 Storage Safety Measures

In order to guarantee the **integrity, confidentiality and availability of information** , NIVALIS DIGITAL SERVICES LLC implements appropriate technical and organizational controls :

a) Digital Security and Encryption

- Databases encrypted with AES-256 standards .
- Restricted access to the Compliance Officer and authorized personnel only .
- Multi -factor authentication (MFA) for system access.

b) Backup and Redundancy

- Backup on independent and secure servers (cloud & on-premise).
- Periodic review of file integrity and automatic recovery in the event of data loss or corruption .

c) Physical Security

- Physical files (where available) stored in locked areas .
- Physical access control to offices with camera monitoring .

11.4 Protection of Personal Data

NIVALIS DIGITAL SERVICES LLC recognizes that the responsible handling of personal information is an essential component of its compliance model. Therefore, it implements data protection policies that cover:

a) Informed Consent

- Each customer must accept the privacy policy before providing their data.
- Consent is digitally documented and becomes part of the client's file.

b) Limited Use

- Personal information is used solely for purposes related to due diligence, monitoring, and compliance reporting.
- It is not shared with third parties, except at the explicit request of competent authorities or contracted suppliers with confidentiality clauses .

c) Rights of the Owner

- The client has the right to request access, rectification or deletion of their data, unless there is a legal obligation to retain it.
- Applications are processed within a maximum period of 30 days .

11.5 International Data Transfer

In cases where customer data must be processed or stored outside of Nevis (through the use of international cloud services), NIVALIS DIGITAL SERVICES LLC guarantees that:

- The servers are located in **jurisdictions that offer an adequate level of data protection , in accordance with internationally recognized** adequacy decisions .
- **Data processing agreements (DPAs)** have been signed with suppliers ensuring compliance with confidentiality, security, and restricted access obligations.

11.6 Internal Oversight on Conservation and Privacy

The Compliance Officer of NIVALIS DIGITAL SERVICES LLC is responsible for:

- Monitor compliance with data retention and processing policies .
- Evaluate every six months the need to retain, destroy or anonymize files.
- Coordinate internal audits on access to sensitive information .
- Document any incident related to leakage, alteration or improper access to data.

11.7 Secure Disposal of Information

At the end of the legal or voluntary retention period, the documentation is eliminated using secure methods :

- Digital files: **certified and unrecoverable erasure** , following industry security protocols (DoD 5220.22-M or equivalent).
- Physical documents : **mechanical destruction using an industrial shredder of level 4 or higher** .

The elimination is recorded in an internal record indicating the date, person responsible and method used.

11.8 Commitment to Transparency and Active Protection

NIVALIS DIGITAL SERVICES LLC believes that orderly record keeping and effective protection of personal data not only serve an internal control function, but also reinforce **the confidence of the client, its banking partners and its international suppliers** .

This commitment is reflected in:

- The existence of written and auditable policies .
- Voluntary cooperation with payment providers and counterparties that request documentary verification .
- Implementing a continuous improvement approach to cybersecurity and compliance .

12. INTERNAL CONTROL BODIES AND FUNCTIONS

At NIVALIS DIGITAL SERVICES LLC, the internal control structure is essential to ensure the proper implementation , monitoring , and continuous improvement of anti -money laundering (AML) and counter-terrorism financing (CFT) policies . To this end, specific bodies and managers with clearly defined roles are established to ensure regulatory compliance and business integrity.

12.1 Internal Control Structure

The internal control structure of NIVALIS DIGITAL SERVICES LLC is composed of:

- **The Compliance Officer**
- **The Compliance Committee (when applicable)**

- **Senior Management**
- **The Operational and Administrative Staff**

12.2 Functions and Responsibilities

a) Compliance Officer

The Compliance Officer is primarily responsible for ensuring the correct execution of KYC & AML policies and procedures within the company, and acts as a liaison with regulatory and financial authorities.

Main responsibilities:

- Oversee the implementation and updating of the KYC & AML Compliance Manual.
- Coordinate ongoing training of staff in the prevention of money laundering and terrorist financing.
- periodic risk assessments to adjust internal controls.
- Monitor operations and review suspicious transactions.
- Submit internal and external reports to the competent authorities when required.
- Maintain up-to-date customer records and due diligence documentation .
- Supervise the conservation and protection of records.
- Conduct internal audits to verify compliance with policies .
- Maintain constant communication with banks, suppliers and other counterparties.
- Manage and document AML/CFT-related incidents or non-compliance.
- Propose corrective and continuous improvement measures.

The Compliance Officer must have functional independence, direct access to senior management , and sufficient authority to implement the necessary measures.

b) Compliance Committee

Depending on the size and operational complexity, NIVALIS DIGITAL SERVICES LLC may form a Compliance Committee , comprised of key members of management and operational areas , which meets periodically to :

- Review and approve policies and procedures related to AML/CFT.
- Analyze reports from the Compliance Officer.

- Evaluate associated operational and regulatory risks.
- Make decisions on disciplinary and preventive measures.
- Oversee the implementation of internal and external audit recommendations .
- Coordinate training and awareness initiatives .

c) Senior Management

Senior management (owners, managers or directors) of NIVALIS DIGITAL SERVICES LLC has the ultimate responsibility for :

- Approve and support the AML and KYC policy .
- technological and financial resources for compliance.
- Ensure that the organizational culture promotes ethics , transparency and compliance.
- Oversee the performance of the Compliance Officer and the Committee .
- Ensure that recommendations and corrective measures are implemented in a timely manner.
- Ensure that the company's operations comply with local and international regulations.

d) Operational and Administrative Personnel

All staff, including customer service , administration and operations areas , must be properly trained to:

- Identify signs or warning signals that may indicate risks of money laundering or terrorist financing.
- Comply with established due diligence and monitoring procedures.
- Report any suspicion or anomaly to the Compliance Officer immediately.
- Actively participate in training and updates.
- Respect the confidentiality and protection of information .

Internal Communication Channels

To ensure effective communication and reporting of incidents, NIVALIS DIGITAL SERVICES LLC establishes:

- A formal internal channel for reporting suspicious transactions and potential non-compliance (secure email , ticketing system, or internal platform).
- Periodic meetings between the Compliance Officer and senior management to assess risks and corrective actions.
- Quarterly or semi-annual reports on the effectiveness of the compliance program.

12.4 Independence and Authority

The Compliance Officer must have sufficient autonomy to perform his or her duties without interference, with the ability to :

- Access all the necessary information .
- Recommend the temporary suspension of suspicious operations.
- Request resources and support for compliance.
- Report directly to senior management or the board of directors .

12.5 Evaluation and Continuous Improvement

Internal control is subject to periodic reviews that include:

- Independent internal audits to evaluate the effectiveness of AML / KYC policies .
- Annual review and update of the Compliance Manual.
- Incorporation of best practices and regulatory recommendations.
- Adjustments to the organizational structure based on growth or changes in the business.

12.6 Incident and Action Log

A formal and confidential record is kept of:

- All alerts received and reports of suspicious transactions.
- Internal investigations carried out.
- Corrective measures taken.
- Training provided .

This record must be available for audits and supervision .

12.7 Culture of Compliance

NIVALIS DIGITAL SERVICES LLC fosters an organizational culture based on:

- Professional ethics .
- Transparency and responsibility.
- Commitment to the prevention of financial crimes.
- Continuous training and team awareness .

This culture is key to ensuring that all members understand their role in preventing money laundering and terrorist financing.

13. STAFF TRAINING AND AWARENESS

Ongoing staff training and awareness is an essential pillar of NIVALIS DIGITAL SERVICES LLC's anti -money laundering and counter-terrorism financing (AML/CFT) policy. A properly informed team aware of the risks and procedures contributes effectively to the early detection and proper management of risks associated with illicit activities .

13.1 Training Objectives

- **Update your knowledge** of AML, KYC, and applicable regulations both locally (Nevis) and internationally.
- **Strengthen the culture of compliance** and ethics within the organization .
- **Improve the ability to identify suspicious** activities and behaviors .
- **Ensure compliance with internal procedures** to mitigate legal and reputational risks.
- **Facilitate the correct application of the** controls established in the Compliance Manual.
- **Promote effective communication** and timely reporting of suspicious or unusual transactions.

Scope of Training

All employees, directors, external collaborators and personnel with access to sensitive information or involved in customer relations are required to participate in AML/CFT-related training programs, including :

- Administrative and operational staff.
- Compliance officers and supervisors.

- Customer service teams .
- Critical service providers and collaborators .

13.3 Training Modalities

NIVALIS DIGITAL SERVICES LLC implements different modalities to adapt to the needs and availability of staff:

- Periodic in-person or virtual **sessions** taught by AML/KYC experts.
- **Online courses and webinars** with updated content and flexible access.
- **Self-study materials** , including manuals, guides , videos, and presentations.
- **Drills and practical exercises to** reinforce the application **of** procedures .
- **Newsletters and internal communications** with regulatory updates and case studies.

13.4 Frequency and Programming

- **Induction** : All new employees must receive training on AML /KYC policies within the first **15** days of joining .
- **Periodic training** : **At** least once a year , mandatory refresher sessions are held for all staff.
- **Special Training:** In the event of major regulatory changes or the identification of new threats, additional sessions are scheduled.
- **Assessments:** Tests or evaluations are administered to measure staff understanding and commitment to policies .

13.5 Basic Training Contents

Training includes, but is not limited to:

- Basic concepts and legal framework of AML and CFT.
- Internal due diligence and monitoring procedures.
- Identification of warning signs and patterns of suspicious behavior .
- Correct use of monitoring systems and tools.
- Suspicious transaction reporting protocol.
- Data protection and confidentiality .

- Individual responsibilities and consequences of non-compliance.
- Practical cases and relevant experiences in the sector.

13.6 Evaluation and Monitoring

To ensure the effectiveness of the training program , evaluation and monitoring mechanisms are implemented:

- Detailed record of attendance and participation .
- Knowledge assessments through questionnaires and tests.
- Feedback and satisfaction surveys .
- Monitoring the practical application of knowledge in daily work.
- Periodic reports to the Compliance Officer and Senior Management .

13.7 Training Responsibilities

- **Compliance Officer: Coordinates, oversees, and updates the** training program , as well as the selection of materials and suppliers.
- **Senior Management : Supports** and promotes a culture of compliance through resource allocation and commitment to ongoing training .
- **Staff:** Actively participate in training and apply what they have learned in their roles.

13.8 Continuous Awareness

Beyond formal training , NIVALIS DIGITAL SERVICES LLC promotes a culture of awareness through :

- Regular communications on new threats and regulatory changes.
- Periodic reminders about the importance of complying with policies .
- Open spaces for questions, doubts and suggestions.
- Promotion of ethical values and corporate responsibility .

13.9 Program Update

training program is reviewed and updated annually to incorporate:

- Local and international regulatory changes.

- New trends and emerging risks in money laundering and terrorist financing.
- Improvements derived from internal audits and evaluations.
- Feedback received from participants and senior management .

13.10 Documentation and Registration

An updated file is maintained with:

- Training plans and programs .
- Attendance lists.
- Evaluation results.
- Materials and resources used.
- Certificates of participation , where applicable.

This documentation is available for audits and supervision .

14. INDEPENDENT REVIEW AND AUDIT

review and auditing are an essential component of NIVALIS DIGITAL SERVICES LLC's internal control system to ensure the effectiveness of and compliance with anti-money laundering and counter-terrorism financing (AML/CFT) policies and procedures . These activities identify areas for improvement, ensure proper implementation of the program, and strengthen the company's compliance culture.

14.1 Objectives of the Independent Review and Audit

- Evaluate the adequacy , effectiveness and compliance of established AML/KYC policies , procedures and controls.
- Detect potential vulnerabilities, non-compliance or deficiencies in the application of the program.
- Verify the correct implementation of previous recommendations and corrective measures.
- Ensure the transparency and reliability of processes related to the prevention of money laundering and terrorist financing.
- Provide objective and detailed information to senior management and regulatory bodies .
- Strengthen the organizational culture of compliance and risk mitigation .

14.2 Scope of the Audit

The audit covers all areas , processes and controls linked to AML/CFT policies , including but not limited to:

- Review of the organizational structure and responsibilities .
- Evaluation of customer due diligence (CDD) and enhanced due diligence (EDD) processes .
- Analysis of transaction monitoring and reporting of suspicious transactions .
- Verification of compliance with internal policies and applicable regulatory standards.
- Review of the technological systems and platforms used for monitoring and control.
- Evaluation of the staff training and awareness program .
- Review of documentation and compliance records.
- Review of communications with regulatory and financial authorities.

14.3 Periodicity and Programming

- The independent audit must be carried out at least once a year .
- Additional audits may be scheduled in the event of incident detection , significant regulatory changes, or at the request of senior management .
- audit schedule must be approved by senior management and coordinated with the Compliance Officer.
- The results of each audit must be presented and discussed with senior management and the Compliance Officer to define actions.

14.4 Auditors and Qualification

- The audit must be conducted by independent professionals with proven experience in AML/CFT and regulatory compliance.
- It can be carried out by specialized internal auditors or by external firms that guarantee objectivity and impartiality.
- Auditors must have full access to the information and documentation necessary to conduct a thorough analysis .

14.5 Audit Process

The process includes:

- **Planning** : Definition of scope, objectives **and** methodology .
- **Execution** : Document review , interviews with key personnel, control tests and **data** analysis .
- **Report**: Preparation of a detailed report that includes findings, observations, detected risks and recommendations.
- **Presentation** : Sharing of the report with senior management and **the** Compliance Officer.
- **Monitoring**: Supervising the implementation of recommendations and corrective actions within established deadlines.

14.6 Reports and Communication

- Audit reports must be clear, objective and contain practical recommendations .
- They must contain an executive summary, description of the methodology , findings, potential impact and proposals for improvement.
- The results will be formally communicated to senior management , the Compliance Officer and, if applicable, to regulatory bodies .
- If serious non-compliance is identified, immediate measures must be taken to mitigate risks .

14.7 Monitoring and Continuous Improvement

- NIVALIS DIGITAL SERVICES LLC will establish mechanisms for the effective monitoring of corrective actions arising from audits .
- The Compliance Officer will be responsible for coordinating and reporting progress to senior management .
- Continuous improvement will be encouraged through periodic updating of policies , procedures and controls based on audit results .
- Auditing is a strategic tool to strengthen the integrity, transparency and reputation of the company.

14.8 Confidentiality

- The entire audit process will be carried out in strict compliance with the confidentiality of the information .
- Auditors and the personnel involved are required to maintain the confidentiality of the data to which they have access.

- Sensitive information will only be shared with authorized persons and according to established procedures.

14.9 Documentation and Archive

- All reports, evidence and documents related to the audits performed will be kept .
- This documentation will be available for internal review and for submission to regulatory authorities if required.
- Records must be kept for the period established by applicable regulations and internal policies .

15. ANNEXES

The annexes are an integral part of the NIVALIS DIGITAL SERVICES LLC KYC & AML Compliance Manual and contain complementary documents, forms, procedures and references that support the implementation and effective operation of the money laundering and terrorist financing prevention program .

15.1 List of Included Annexes

The following documents and materials are attached to facilitate the understanding and application of the policies and procedures described in this manual:

15.1.1 Customer Due Diligence (CDD) and Know Your Customer (KYC) Forms

Introduction

Customer Due Diligence (CDD) and Know Your Customer (KYC) forms are essential tools for collecting and documenting the information necessary to identify, verify, and evaluate NIVALIS DIGITAL SERVICES LLC customers. These forms help us comply with regulatory requirements, prevent illicit activities , and properly manage the risks of money laundering and terrorist financing.

Objectives of the form

- Collect clear, accurate, and verifiable information about the client's identity, economic activity , and source of funds.
- Establish the client's risk profile to apply proportional controls.
- Document compliance with applicable legal and regulatory requirements in Nevis and relevant international jurisdictions.
- Facilitate the detection of warning signs that may indicate suspicious activities .

Form content

The main sections that must be included in the CDD/KYC form are described below :

1. General Customer Information

- **Full name or company name :**
- **Type of person:** (Natural / Legal)
- **Date of birth or incorporation :**
- **Nationality or country of incorporation :**
- **Official identification number or commercial registry :**
- **Physical and postal address :**
- **Telephone number and email address :**

2. Documentation required for verification

- Legible copy of official identity document (passport, ID card , license, etc.) for natural persons.
- Constitutive documents and bylaws for legal entities .
- Certificate of good reputation or non-existence.
- Recent proof of address (utility bill, bank statement, etc.) dated no more than 3 months ago.

3. Information on Economic Activity and Source of Funds

- description of the client's economic or commercial activity .
- Origin and source of the funds with which the operations will be carried out .
- Estimated volume and frequency of planned operations.

4. Final beneficiaries and corporate structure

- Identification of beneficial owners with significant stakes in the company (for example, those who own more than 25% of the shares or control).
- List of directors, agents and legal representatives .

5. Risk Assessment

- Identification of risk factors (jurisdiction , activity, type of client).
- Preliminary classification of the client into risk categories (low, medium, high) .
- Justification and additional comments.

6. Declarations and Consents

- Customer declaration regarding the veracity of the information provided .
- Consent for the processing and storage of personal data in accordance with the privacy policy .
- Authorization to perform additional checks (sanctions lists, PEP lists, public databases , etc.).

Procedure for filling and verification

- The form must be completed by the client or by authorized personnel of NIVALIS DIGITAL SERVICES LLC, ensuring that all required documentation is obtained .
- The information must be verified with the documents provided and, where necessary, through independent sources or reliable databases.
- If inconsistent information or missing documents are detected, clarification or additional documentation must be requested before approving the business relationship .

Confidentiality and conservation

- The collected forms and documents will be stored under strict security measures to ensure the confidentiality of the information .
- They will be kept in accordance with the time limits established in the manual and applicable regulations.

15.1.2 Procedure for the Identification and Reporting of Suspicious Operations (ROS)

Introduction

NIVALIS DIGITAL SERVICES LLC is committed to rigorously complying with current legal and regulatory provisions regarding the prevention of money laundering and counter-terrorism financing (AML/CTF). A fundamental part of this commitment is the implementation of a clear and

effective procedure for the timely identification and reporting of suspicious transactions (STRs), with the goal of preventing and detecting potential illicit activities .

Objectives of the procedure

- Detect activities or transactions that may indicate the possible commission of money laundering, terrorist financing, or other related crimes.
- Establish an internal protocol for the evaluation , documentation and reporting of suspicious transactions.
- Ensure compliance with Nevis regulatory requirements and international standards .
- Protect the integrity, reputation and operation of NIVALIS DIGITAL SERVICES LLC.

Definition of Suspicious Operation

A suspicious transaction is considered to be any transaction , behavior or pattern of conduct that, due to its characteristics or circumstances, raises reasonable doubts about its legality or integrity, including, but not limited to :

- Transactions without clear economic or commercial justification .
- Complex, unusual or excessively large operations for the client profile.
- Repeated use of accounts or payment methods in jurisdictions considered high risk.
- Inconsistent information or attempt to conceal identity or beneficiaries.
- Clients who refuse to provide required documentation or information .
- Transactions linked to persons or entities included in sanctions lists or politically exposed persons (PEPs).

Procedure for identifying suspicious transactions

1. **Continuous Monitoring:**
Authorized personnel will constantly monitor customer operations and activities to detect any anomaly or suspicious indication.
2. **Red Flag Detection :**
Checklists , indicators, and risk assessment tools **will** be used to identify atypical patterns .
3. **Preliminary investigation :**
Upon detection of a possible suspicious operation , a detailed review will be carried out , including consultation with the client to clarify doubts or inconsistencies.

4. **Documentation** : Every suspicious operation must be carefully documented, recording data, reasons for suspicion, analyses performed and results obtained.

Internal report

- If reasonable doubts persist after the preliminary investigation , the case must be reported immediately to the Compliance Officer.
- The Compliance Officer will evaluate the information and decide whether to submit the report to the competent authority.
- The internal report must include:
 - Data of the client involved
 - Detailed description of the operation or suspicious behavior
 - Preliminary analysis and conclusions
 - Supporting documentation

Report to the authorities

- The Compliance Officer will make the official report to the corresponding regulatory or financial authority in Nevis, complying with the established timeframes and formats.
- confidentiality will be maintained throughout the process to protect those involved and avoid undue harm.
- will not be informed about the report so as not to compromise the investigation or violate confidentiality rules.

Training and awareness

- All personnel must receive periodic training to recognize warning signs and know the procedure for reporting suspicious transactions.
- An internal culture of compliance and responsibility will be promoted .

Confidentiality and protection

- Information related to suspicious transactions will be handled with strict confidentiality.
- will be implemented to protect data and prevent unauthorized disclosure.

Review and continuous improvement

- The identification and reporting procedure will be reviewed regularly to incorporate best practices and respond to regulatory changes.
- All cases and actions will be documented for internal and external audits .

AML/CFT Risk Assessment Matrix

Introduction

The AML/CFT Risk Assessment Matrix is a fundamental tool for NIVALIS DIGITAL SERVICES LLC to identify, analyze, and manage the risks associated with the prevention of money laundering and terrorist financing. This matrix allows for a periodic and objective assessment of the risks inherent to clients, products, services, and jurisdictions with which the company interacts, facilitating the prioritization of controls, monitoring, and effective preventive actions.

Goals

- Systematically assess the risk levels related to the company's business activities and relationships.
- Identify critical areas that require greater attention and strengthened controls.
- Facilitate risk-based decision-making to optimize resources and compliance efforts.
- Comply with Nevis' regulatory obligations and international standards regarding AML/CFT.

Components of the Risk Assessment Matrix

The matrix is designed to assess four main risk categories :

1. **Customer**

Risk:
The customer profile is assessed considering their economic activity , geographic location , history, level of transparency and relationship with politically exposed persons (PEP).
2. **Product/Service**

Risk:
The products and services offered are analyzed, identifying those that by their nature may be more vulnerable to illicit uses , such as digital services, electronic payments or any product that facilitates complex or anonymous transactions .
3. **Jurisdiction**

Risk :
Jurisdictions where clients operate or funds originate are assessed, taking into account factors such as local regulation, international reputation , lists of high-risk or non-cooperative countries , and the presence of deficient AML measures.

4. Transactional

Risk:

Includes the frequency, volume and complexity of transactions, the speed and type of channels used for the transfer of funds or provision of services.

Methodology for assessment

Each category is evaluated by assigning a risk level that can be low, medium or high, according to predefined criteria and documentary evidence.

Risk Level	Description	Recommended Actions
Low	Client/product/jurisdiction with low risk potential	Standard controls and regular monitoring
Half	Moderate risk, requires special attention	Reinforced controls and more frequent periodic review
High	High risk that could involve significant exposure	Enhanced due diligence (EDD), ongoing monitoring and potential restrictions

Periodic evaluation process

1. Information collection

:

Up -to - date data is collected on customers, products, jurisdictions, and transactions.
2. Application of the matrix:

The Compliance Officer applies the matrix for each client and activity, assigning risk levels according to the established criteria.
3. Recording and documentation

:

The results of the evaluation are documented in an internal record, including the decisions made and the measures applied.
4. Continuous update

:

The matrix and assessments are reviewed at least once a year in response to any relevant changes in the operation or regulatory context.

Benefits of the Risk Assessment Matrix

- Improves effectiveness in preventing money laundering and terrorist financing.
- It enables proactive and evidence-based risk management .
- Facilitates the efficient allocation of compliance resources.
- Strengthens trust with financial institutions, business partners, and regulatory authorities.

15.1.4 List of High Risk Jurisdictions and Sanctioned Entities **Reference and Control Instrument**

This document is an integral part of **NIVALIS DIGITAL SERVICES LLC 's AML/CFT system** and is used to identify countries , territories, or entities at high risk for money laundering, terrorist financing, and evasion of international sanctions. Its maintenance is mandatory, and its periodic review is the responsibility of the Compliance Officer.

International Sources

The preparation and updating of this list takes into account the following official sources :

- Financial Action Task Force (**FATF**)
- U.S. Office of Foreign Assets Control (**OFAC**)
- United Nations Security Council (**UN**)
- European Union (**EU**)
- HM Treasury of the United Kingdom
- Regional lists of the Caribbean and Latin America

1. FATF Jurisdictions

Blacklist (high risk, reinforced measures):

- **North Korea**
- **Go to n**
- **Myanmar (Burma)**

Grey List (intensified monitoring):


- Barbados
- Burkina Faso
- Cameroon
- Croatia
- Haiti
- Jamaica
- Kenya

- Mali
- Mozambique
- Nigeria
- Philippines
- Senegal
- South Africa
- South Sudan
- Syria
- Tanzania
- Turkey
- Uganda
- **United Arab Emirates**
- Yemen
- Vietnam

2. Jurisdictions with active international sanctions (OFAC, UN, EU):

- **Afghanistan**
- **Belarus**
- **Cuba**
- **Go to n**
- **Lebanon**
- **Libya**
- **Nicaragua**
- **North Korea**
- **Russia**
- **Syria**
- **Venezuela**

- **Yemen**
- **Zimbabwe**

 **Russia is subject to sectoral and comprehensive financial sanctions by the US, EU, UK and other countries due to** military actions, AML/CFT control deficiencies and sanctions evasion .

3. EU list of non-cooperative tax havens (2024):

- Fiji
- Guam
- US Virgin Islands
- Palau
- Panama
- **Russia**
- Samoa
- American Samoa
- Trinidad and Tobago
- Turks and Caicos Islands
- Vanuatu

Internal measures at NIVALIS DIGITAL SERVICES LLC

- Any match with a listed jurisdiction triggers an **Enhanced Due Diligence (EDD)** alert .
- Relations with entities or persons under total sanction are prohibited .
- justification from the Compliance Officer is required in the case of exceptions permitted under economic or legal criteria.
- This list is updated **monthly** , and shared with all staff involved in onboarding, compliance and monitoring.

15.1.5 Data Protection and Confidentiality Policies

General Objective

purpose of this policy is to establish the principles, guidelines and procedures for the collection , storage, processing, access, transmission and elimination of personal and confidential data of clients, employees, suppliers and any third party linked to **NIVALIS DIGITAL SERVICES LLC** , guaranteeing its security, confidentiality, integrity and availability, in compliance with the best international practices and regulations on data protection .

1. Guiding Principles

data protection policies are governed by the following principles :

- **Legality, fairness and transparency** : Data is processed on a legal basis, in a fair and transparent manner with the owner.
- **Purpose limitation** : Data is collected for legitimate , explicit and **clearly** defined purposes.
- **Data minimization** : Only data strictly necessary for the stated purpose **is** collected .
- **Accuracy** : Reasonable steps are taken to ensure that data is up to date and accurate.
- **Storage limitation** : Data will not be **retained** longer than necessary .
- **Integrity and confidentiality** : **Appropriate** technical and organizational measures are adopted to protect data against unauthorized or unlawful processing , loss , destruction or accidental damage .

2. Scope

This policy applies to:

- Customer information (identification , **address** , KYC documents , transaction history, communications).
- Employee **and contractor** information (personal , employment and financial data).
- Information on suppliers **and business partners** .
- Any other sensitive or confidential data handled by NIVALIS DIGITAL SERVICES LLC.

3. Obligations of the Company

NIVALIS DIGITAL SERVICES LLC is committed to:

- technical and organizational measures to protect personal and sensitive data.
- Inform the data subject about the processing of their data and obtain their consent, where appropriate.

- Ensure that only authorized personnel have access to confidential information .
- Conduct periodic audits and risk assessments on information security .
- risk management protocols and, if applicable, to the relevant authorities .
- Implement secure data retention and destruction policies in accordance with legal and contractual deadlines.

4. Data Management and Access

- Access to confidential information is granted on a **need-to-know basis** .
- All staff must sign a **confidentiality agreement** as part of their onboarding .
- Encrypted systems and secure platforms are used for digital storage and data transmission .
- Physical files with personal data are stored in places with controlled and restricted access.

5. International Data Transfers

In the event that cross-border data transfers are required, NIVALIS DIGITAL SERVICES LLC:

- will ensure that the receiving country has adequate **levels of protection , according** to international standards (such as the General Data Protection Regulation – **GDPR**).
- Use **data processing agreements (DPAs) and** standard contractual **clauses (SCCs)** where appropriate.
- Ensure that any third party receiving the data complies with the confidentiality and protection principles established in this policy .

6. Rights of the Data Subject

Every data subject has the right to:

- Access your personal information .
- Request the rectification or deletion of your data.
- Restrict or object to the processing of your data in certain cases.
- Receive a copy of your data in digital format (portability).

To exercise these rights, you can contact the Compliance Officer by email **at** **compliance@nivalisdigital.com** .

7. Training and Awareness

Staff are regularly trained on compliance with data protection and confidentiality regulations. In addition , a culture of **digital responsibility and information ethics is promoted** .

8. Non-compliance and Sanctions

Any breach of this policy will be assessed based on the severity of the incident and may result in disciplinary action, including termination of employment and notification to the appropriate authorities if applicable.

15.1.6 Training and Awareness Record

General Objective

The purpose of this annex is to establish a formal and documented system to record, verify and evaluate the participation of NIVALIS **DIGITAL SERVICES LLC personnel in** training , capacity building and awareness-raising activities related to the prevention of money laundering (AML) and combating the financing of terrorism (CFT), in accordance with international standards , FATF recommendations and compliance principles voluntarily adopted by the company as part of its ethical commitment and institutional responsibility.

1. Justification

Although NIVALIS DIGITAL SERVICES LLC is not bound by a licensing regime for financial activities, the company implements a proactive **compliance policy , adopting internal** training mechanisms to strengthen the organizational culture against the risk of money laundering and terrorist financing , especially in international environments where operational credibility depends on institutional and staff behavior.

2. Formats and Records Used

Various standardized documents are used to monitor the training process. The main ones are:

- **Training Attendance Form .**
- **AML/CFT Knowledge Assessment Record (pre and post training) .**
- **Training Plan .**
- **Certificates of Participation .**
- **Participation and Performance Indicators Report .**

All of these documents are digitally archived and backed up in secure storage systems under the control of the Compliance Officer.

Minimum Content of Records

Each record must include at least:

- Full name of the participant.
- Position and operating unit.
- Date of training .
- Course topic and objectives.
- Modality (in person, virtual, asynchronous).
- Facilitator or training entity.
- Participant's signature or electronic validation .
- Evaluation result (if applicable).
- Participant's comments or observations.

4. Types of Training Considered

- **Initial Training** : Aimed at all staff upon joining the company, to familiarize themselves with **internal** compliance policies .
- **Continuous Training** : Periodic sessions **to** update knowledge, especially in response to regulatory or risk changes.
- **Targeted Training** : **Aimed at sensitive or high -** impact positions in the due diligence process.
- **Drills or practical exercises** : Fictional cases on suspicious transactions, enhanced due diligence or risk assessment .

5. Responsibilities

- **Compliance Officer (MLRO)** : Responsible for designing the annual training plan , managing external providers, maintaining records and preparing reports for senior management .
- **Human Resources Area** : Provides support in the planning and logistical monitoring of training events.

- **Employees and Contractors** : They have the responsibility to attend, actively participate in and pass the required training.

6. Evaluation and Monitoring

Assessment tools (questionnaires, surveys, quick tests) are used to measure content comprehension and retention . Employees who do not meet the minimum criteria will be called in for reinforcement sessions.

Additionally, management reviews training indicators quarterly and approves corrective measures when coverage or effectiveness are insufficient.

7. Record Keeping

All records related to AML/CFT training activities are retained for a minimum period of 5 years , **whether** in physical or electronic format , in a secure , confidential manner and accessible only to authorized personnel.

Internal Reports and Audit

- The Compliance Officer generates an annual training and awareness performance report for senior management.
- These records will be available for inspection by internal or external auditors, and may be included in **banking due diligence processes** or **international regulatory inspections** , if applicable.

Internal and External Audit Procedure

General Objective

Establish a clear, systematic and documented procedure for conducting internal and external audits on the prevention of money laundering (AML) and terrorist financing (CFT), which guarantees the identification of deficiencies, the follow-up of recommendations and the continuous improvement of the policies and controls adopted by **NIVALIS DIGITAL SERVICES LLC** .

1. Guiding Principles

Audits are based on the following principles:

- **Independence** : Internal audits are conducted by personnel not directly involved in the execution of AML/CFT controls; external audits are carried out by qualified, independent third parties.

- **Frequency** : At least one internal audit per year and one external audit every two years , or when determined by senior management .
- **Objectivity** : Evaluations based on documented evidence, free from subjective judgments.
- **Confidentiality** : All audited information and its results are handled under strict confidentiality criteria.

2. Scope of the Audits

Audits include , but are not limited to:

- AML/CFT Policies and Procedures .
- Risk assessment and risk matrix.
- Due diligence records (CDD and EDD).
- Processes for monitoring and reporting suspicious transactions.
- Staff training .
- Data records and their protection .
- Compliance supervision by the Compliance Officer.
- Integrity of documentation and compliance reports.

the Audit Process

3.1 . Planning

- Definition of objectives and scope .
- Identification of the processes to be audited.
- Assignment of internal auditors or hiring of an external firm.
- Advance request for relevant information .

3.2 . Execution

- Review of internal policies and documents .
- Interviews with the Compliance Officer and key employees.
- Verification of customer records, ROS reports and risk matrix .

- Evaluation of compliance with previous recommendations.

3.3. Preparation of the Report

- Presentation of findings with clear evidence.
- Classification of detected risks (high, medium, low).
- Concrete recommendations with deadlines for implementation .
- Compliance culture assessment and training .

3.4. Presentation to the Management

- Delivery of the complete report to the Compliance Committee or senior management .
- Discussion of findings and approval of corrective action plan .

3.5. Monitoring

- Record of progress in the implementation of improvements.
- Verification audits when there are critical findings that have not been corrected.
- Inclusion in future audits to review recurrences.

4. Procedure Managers

- **Chief Compliance Officer (MLRO)** : Coordinates internal audits and is the point of contact for external audits .
- **General Management : Approves** audit plans and allocates resources.
- **Internal Auditors or External Firm** : They carry out the audit independently and impartially.
- **All Staff** : Collaborate by providing the requested information and documentation .

5. Procedure Documentation

The following documents and forms are part of the procedure:

- **Annual AML/CFT Audit Plan** Format .
- **Internal Auditor** Checklist .
- **Auditor Report** Format .
- **Findings and Corrective Actions Matrix** .

- **Audit Trail Record .**

6. Conservation and Availability of Records

Audit reports , checklists and follow - up records are retained for a minimum of **5 years** , and will be available for review by correspondent banks, commercial counterparties or legal processes if required , under a confidentiality protocol.

7. Voluntary External Auditor

Although the company has no regulatory obligations in Nevis as it is not subject to a financial license, **NIVALIS DIGITAL SERVICES LLC** may voluntarily submit to AML/CFT audits conducted by internationally recognized independent firms, as a measure of transparency and reputational strengthening .

8. Checklist Model for AML/CFT Internal Auditor

Below is a sample checklist used by internal auditors :

Area Evaluated	Complies (Yes / No)	Evidence Review	Observations
Existence of AML/KYC policies			
Complete customer registration			
Risk assessment by client			
EDD procedures applied			
Recent training recorded			
Record of unusual transactions			
Control of sanctioned lists			
Prior corrective actions			

15.1.8 Document Conservation and Archiving Policy

Aim

adequate conservation , filing, access, and eventual secure destruction of documents related to compliance with the anti -money laundering and terrorist financing (AML/CFT) program at **NIVALIS DIGITAL SERVICES LLC** , as part of its commitment to transparency, traceability and corporate responsibility.

1. Scope

This policy applies to all physical and digital documentation generated or received by NIVALIS DIGITAL SERVICES LLC in the course of its compliance activities, including:

- Customer identification documentation (KYC) .
- Results of risk assessments (CDD and EDD).
- Suspicious transaction reports (SARs).
- Checklists and correspondence with international organizations.
- Staff training and awareness records .
- Audit reports and follow-up.
- Risk matrices and internal controls applied.

2. General Principles

- **Integrity and authenticity** : Documents must be kept in a way that ensures their integrity, avoiding alterations or loss of information .
- **Accessibility and localization : Documentation** must be organized and accessible for consultation by the competent authorities, correspondent banks or auditors.
- **Security and confidentiality** : Technical and administrative measures must be adopted to prevent unauthorized access, leaks or misuse.
- Defined **temporality** : Each document will have a minimum conservation period defined in this policy , in accordance with international good practices .

3. Conservation Periods

Document Type	Conservation Minimum
KYC, CDD and EDD forms	5 years since the closing of the commercial relationship
Suspicious Transaction Reports (STRs)	5 years since the generation of the report
Internal and external audit documents	5 years since the audit
Training records	5 years since the training activity
Correspondence with clients or authorities	5 years from the date of issue or receipt
Risk assessments, matrices and controls	5 years since last update

Storage and Organization

4.1. Physical Archive

- physical file will be kept in secure, locked facilities, with access restricted to authorized compliance personnel .
- Each file must be classified by client number, date or document type, as established in the internal file manual.

4.2. Digital Archive

- physical documents must be scanned and stored in an encrypted, automatically backed-up digital system .
- Access to the digital file will be limited by credentials assigned by the Compliance Officer.
- Periodic backups (at least weekly) must be made on encrypted media.

5. Secure Document Destruction

Once the defined retention period has elapsed , the documents will be securely deleted or destroyed, ensuring that they cannot be recovered or misused.

5.1 Destruction procedure

- **Physical** : Destruction using **high** - security shredders or certified document destruction services.
- **Digital** : Deletion using secure erasure software (wiping) that prevents recovery .

The destruction must be documented with a **Document Elimination Certificate** , signed by the person responsible for the file and validated by the Compliance Officer.

6. Responsibilities

- **Compliance Officer (MLRO)** : Monitor compliance with this policy , authorize document destruction , and maintain retention records .
- **Compliance and Administrative Support Staff** : Classify, file and maintain documents according to established guidelines.
- **Internal/External Auditor** : Verify the existence and status of files during the review processes .

7. Policy Review

This policy will be reviewed and updated annually, or when there are changes in international regulations, filing technology or organizational structure of NIVALIS DIGITAL SERVICES LLC .

15.1.9 Contacts and Communication Channels

Contact information for the Compliance Officer, responsible areas , and regulatory authorities to facilitate timely communication and reporting of any incidents .

1. Objective

communication channels for reporting suspicious activities, inquiries regarding AML/CFT procedures, coordination with authorities, and staff feedback regarding the implementation of the compliance program.

2. Principal Responsible: Compliance Officer (MLRO)

The **Money Laundering Reporting Officer (MLRO)** will be the central point of contact for all matters related to the prevention of money laundering and terrorist financing. He or she will be responsible for receiving, analyzing, and internally escalating any alerts or inquiries related to the AML/CFT program.

Compliance Officer Data

- **Full name** : Inovejas Rowena Estrada
- **Position** : Compliance Officer (MLRO)
- **Email** : compliancennialis@protonmail.com
- **Direct phone number** : +27 65 215 0718
- **Internal encrypted channel** : **Corporate** messaging platform (Signal / Private Telegram)
- **Hours of availability** : Monday to Friday, 9:00 AM to 6:00 PM (UTC-4)

3. Internal Communication

3.1 Internal Incident Reporting (Whistleblowing AML)

- Any staff member can confidentially and directly report any unusual or suspicious behavior or non-compliance with the AML/CFT program.

- anonymous reporting channel is maintained through the encrypted form accessible on the company intranet.

3.2 Communication between Areas

- The Support, Legal, Technology, and Customer Service areas must maintain fluid and constant communication with the Compliance Officer to validate sensitive processes, high-risk clients, or operational changes.

4. External Communication

Although **NIVALIS DIGITAL SERVICES LLC** is not subject to direct supervision by a financial regulatory body in Nevis, it remains available to cooperate with competent authorities in accordance with international cooperation treaties and voluntary compliance standards.

4.1 International Authorities and Sanctions Lists

- The company consults and cooperates with international organizations in the event of warranted investigations, including:
 - **Financial Action Task Force (FATF)**
 - **Office of Foreign Assets Control (OFAC - USA)**
 - **Interpol**
 - **Europol**
 - **Eastern Caribbean Supervisory Body (ECCB) , if applicable.**

4.2 Contact with Banking Entities and External Suppliers

- Any documentary requirements, customer validation, or information requests from correspondent banks, business partners, or payment platforms must be channeled through the Compliance Officer.

5. Response to Official Requests

In the event of receiving formal requests from national or foreign authorities (judicial, police or prosecutors), the following must be done :

- Verify the legitimacy and competence of the request.
- Notify the MLRO and General Management.
- shipping record .

15.2 Updating and Controlling Annexes

- The annexes will be reviewed and updated periodically to ensure that they reflect regulatory changes, international best practices and the specific needs of NIVALIS DIGITAL SERVICES LLC.
- Any updates will be approved by senior management and communicated in a timely manner to all staff.
- The annexes must be consulted and used as a mandatory reference for effective compliance with the manual.

15.3 Use and Access

- The annexes will be available in digital and/or printed format for all personnel involved in the application of the AML/CFT program.
- must be guaranteed to preserve the confidentiality and integrity of the documents.
- The Compliance Officer will be responsible for managing the distribution , updating and storage of the annexes.

16. FINAL STATEMENT AND ADOPTION OF THE MANUAL

This **KYC & AML/CFT Compliance Manual** has been developed and adopted by **NIVALIS DIGITAL SERVICES LLC** , a company incorporated in Nevis, as part of its firm and voluntary commitment to the prevention **of** money laundering , **terrorist financing and other illicit activities that** could compromise its operational or reputational integrity.

Although the nature of NIVALIS DIGITAL SERVICES LLC's business does not require a mandatory license as a financial services or virtual asset provider, the company has decided **to implement robust internal standards** , of international scope, regarding customer identification , transaction monitoring, due diligence and risk control.

This document reflects the organizational structure, procedures and internal policies that guarantee the responsible application of principles of **transparency, traceability, confidentiality and legality** , in line with :

- The recommendations of the Financial **Action Task Force (FATF)** .
- Voluntary compliance standards of international **jurisdictions** .
- The expectations of the **banking, technology, and commercial providers with which** the company maintains relationships .

Validity and Update

This manual comes into force as of May **22**, 2025 , **and** will be reviewed at least once **a year or whenever relevant regulatory changes occur** , substantial modifications in the company's operations occur, or gaps in its implementation are detected .

Updates will be documented in a **review log** included in the company's compliance files and, where necessary, communicated to suppliers and strategic partners .

Obligation of Internal Compliance

All staff members, including managers, external consultants, and temporary collaborators, **are required to understand, comply with, and apply** the guidelines established in this manual. Failure to do so does not exempt them from liability, and failure to comply may lead to disciplinary action or termination of the contractual relationship .

Institutional Commitment

NIVALIS DIGITAL SERVICES LLC recognizes that compliance is not merely a documentary obligation , but a core component of its ethical and sustainable business model . This manual constitutes a living prevention and control tool , which contributes to building trust locally and internationally.

The company reiterates its willingness to cooperate with the competent authorities within the current legal framework, as well as to maintain open, secure, and confidential communication channels for any matter related to the prevention of financial crimes.

Approved

Name: Stefan Eugen

Position: CEO

Date: 04.06.2025

Signature:

Firmado por:

F080EB2EC3FE416...


Validated

Name: Inovejas Rowena Estrada

Position: MLRO

Date: 04.06.2025

Signature:

Firmado por:

19FA6D46D604D8...