ANTI-MONEY LAUNDERING (AML) COMPLIANCE POLICY NEXT SOLUTIONS CORP.

Effective August 5, 2025

1. Purpose and Scope

This Anti-Money Laundering (AML) Policy outlines the internal policies, procedures, and controls adopted by NEXT SOLUTIONS CORP. ("the Company") in compliance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and related regulations issued by **FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)**. This policy applies to all employees, contractors, officers, and directors of the Company.

2. Company Overview

- **Company Name:** NEXT SOLUTIONS CORP.
- **Corporation Number:** 1001042225
- **Address: 155 East Beaver Creek Road, Suite 24-147, Richmond Hill, Ontario, L4B2N1, Canada**
- **Primary Activity (NAICS):** 522329 – Other financial transactions processing and clearing house activities
- **Designated AML Compliance Officer:** Vladimir Kochenov (President & Director)
- **Contact Email:** info@next-solutions.io

3. Governance and Accountability

NEXT SOLUTIONS CORP. is committed to ensuring full compliance with AML/ATF obligations and mitigating risks related to money laundering, terrorist financing, and sanctions violations. The Company:

- Appoints an **AML Compliance Officer** responsible for implementation and oversight of the AML program
- Ensures ongoing **Board-level oversight** of AML compliance
- Maintains clear documentation of all AML-related activities

4. Risk-Based Approach (RBA)

The Company applies a **Risk-Based Approach (RBA)** to all aspects of its anti-money laundering and anti- terrorist financing (AML/ATF) compliance program, including client onboarding, transaction monitoring, and reporting obligations. This approach ensures that resources are allocated effectively, and that higher- risk situations receive enhanced scrutiny and controls.

Key Elements of the Risk-Based Approach:

- **Risk Identification and Assessment**
  The Company identifies and evaluates inherent and residual risks associated with:
  Products and services offered (e.g., electronic transfers, virtual assets, prepaid cards) **Delivery channels** (e.g., online onboarding vs. in-person, use of intermediaries)
  Types of clients (e.g., individuals, corporations, PEPs)
  Geographic risk (e.g., clients located in high-risk jurisdictions or sanctioned countries)
  Transaction behavior (e.g., volume, frequency, velocity, counterparties involved)
- **Risk Classification**
  Based on the assessment, customers and transactions are categorized as:
  Low-risk: standard due diligence applies
  Medium-risk: additional monitoring and periodic review required
  High-risk: subject to **Enhanced Due Diligence (EDD)** and more frequent reviews
- **Enhanced Due Diligence (EDD)**
  For high-risk customers or transactions, the Company implements additional controls, including:
  Obtaining detailed information about the source of funds and wealth
  Verification of beneficial ownership and corporate structure
  Ongoing transaction pattern analysis
  Increased frequency of customer file reviews
  Approval from senior management before entering into a business relationship

- **Risk Scoring System**
  The Company may employ a manual or automated scoring methodology to calculate the composite risk level of a customer based on weighted indicators (e.g., nationality, occupation, transaction profile, etc.).
- **Ongoing Risk Re-Evaluation**
  Customer risk ratings are subject to re-assessment in case of:
    Changes in behavior or transaction patterns
    Trigger events (e.g., adverse media, sanction alerts)
    Periodic scheduled reviews (based on risk category)
- **Mitigation Measures**
  Based on the identified risks, the Company
    may: Restrict access to certain products or
    services Impose transaction limits
    Terminate the business relationship if the risks cannot be mitigated

This dynamic risk-based approach enables the Company to detect, assess, and respond to emerging threats in a timely and proportionate manner.

5. Know Your Customer (KYC) and Client Identification

NEXT SOLUTIONS CORP. ensures that all clients are properly identified in compliance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and related guidance issued by **FINTRAC**. Client identification is a fundamental component of the Company's AML program and is performed both at the time of onboarding and on an ongoing basis throughout the business relationship.

The Company identifies and verifies the identity of every client, whether an individual or a legal entity, before establishing a business relationship or conducting any transaction that meets the reporting thresholds or presents a heightened risk. For individuals, government-issued photo identification (such as a passport or driver's license) is used, along with additional verification measures for remote onboarding (e.g., dual-process method, credit file method, or prescribed technology solutions).

In the case of legal entities, the Company obtains incorporation documents and verifies registration status, business address, and the identities of directors and authorized signatories. Where applicable, the beneficial ownership structure is established and verified, with the identity of any individual who ultimately owns or controls, directly or indirectly, 25% or more of the entity.
KYC obligations are not limited to the initial onboarding phase. The Company performs **ongoing due diligence** by monitoring client transactions for consistency with the stated business purpose and risk profile. Where discrepancies or red flags are identified, enhanced due diligence is triggered. Client records are reviewed and updated periodically, especially for clients classified as medium or high risk.

All identification information and related documentation are retained in accordance with FINTRAC record- keeping requirements and are readily accessible for audit or investigation purposes. Any failure or refusal by a client to provide sufficient identification will result in denial or termination of the business relationship.

6. Record-Keeping Requirements

NEXT SOLUTIONS CORP. maintains detailed and accurate records in accordance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and the applicable **FINTRAC guidance**. All records are retained for a minimum of five (5) years from the date of creation or from the end of the business relationship, whichever is later.
The Company stores copies of all documents used to verify client identity, including the method and result of verification, as well as beneficial ownership information where applicable. Records of the business relationship include the nature and intended purpose of services provided, internal notes on client risk level, and relevant updates over time.

For every financial transaction, the Company maintains a clear audit trail, capturing dates, amounts, currencies, involved parties, payment channels, and references. Where required, the Company also keeps copies of all reports submitted to FINTRAC — including Suspicious Transaction Reports (STRs), Large Cash Transaction Reports (LCTRs), and Electronic Funds Transfer Reports (EFTRs).

In addition, internal records related to compliance decisions, sanctions screening outcomes, and enhanced due diligence are preserved. Employee training logs and audit reports are maintained as part of the compliance documentation.

All records are stored securely, access is restricted to authorized personnel, and retrieval procedures are in place to ensure timely response to audit or regulatory inquiries.

7. Transaction Monitoring and Reporting

NEXT SOLUTIONS CORP. maintains an ongoing process to monitor all transactions for potential signs of money laundering, terrorist financing, or other suspicious or unusual activity. The monitoring framework combines both **automated tools** and **manual oversight**, enabling the Company to identify patterns, trends, and red flags that deviate from the expected behavior of clients.
The Company uses transaction monitoring to detect common money laundering techniques such as structuring (smurfing), rapid movement of funds without an economic rationale, the use of nominee accounts or third parties, frequent large cash deposits, or high-volume transactions inconsistent with the client's profile. Alerts generated by automated systems are reviewed by the Compliance Officer or trained personnel for further investigation and escalation, if necessary.
Where suspicious activity is identified, the Company complies with its obligations to file reports with **FINTRAC**, Canada's financial intelligence unit. These reports include:

- **Suspicious Transaction Reports (STRs):** Filed when there are reasonable grounds to suspect that a transaction is related to the commission or attempted commission of a money laundering or terrorist financing offence.
- **Large Cash Transaction Reports (LCTRs):** Required for cash transactions of CAD $10,000 or more made in a single transaction or in multiple transactions that appear to be related.
- **Electronic Funds Transfer Reports (EFTRs):** Required for international incoming or outgoing electronic funds transfers of CAD $10,000 or more.
- **Terrorist Property Reports (TPRs):** Filed when the Company has property in its possession or control that is known or suspected to be owned or controlled by or on behalf of a listed terrorist entity.

Each report is submitted in accordance with FINTRAC's prescribed timelines and reporting formats. Documentation and rationale for reporting (or not reporting) are retained in internal compliance records for accountability and audit purposes.
The transaction monitoring system is reviewed periodically to ensure it remains effective in detecting evolving typologies and meets regulatory expectations. Updates may include changes in risk indicators, thresholds, or escalation protocols as required by changes in law or the Company's risk environment.

8. Sanctions Compliance

NEXT SOLUTIONS CORP. is fully committed to complying with all applicable **Canadian and international economic sanctions** regulations. This includes sanctions imposed under Canadian law, as well as those issued by international bodies and partner jurisdictions when relevant to the Company's operations.

At a minimum, the Company screens all clients, counterparties, and relevant transactions against the **Consolidated Canadian Sanctions List** maintained by **Global Affairs Canada**. In addition, the Company takes into consideration applicable designations from the **United Nations Security Council (UNSC)**, the **Office of Foreign Assets Control (OFAC, U.S. Department of the Treasury)**, and the **European Union (EU)**, particularly in cases where cross-border activities or international exposure may give rise to elevated sanctions risk.

Sanctions screening is conducted both at the time of onboarding and on an ongoing basis throughout the client relationship. This includes periodic re-screening of existing clients and real-time screening of transactions where applicable. The Company uses automated and/or manual tools to identify potential matches and flags any confirmed or suspected matches for review by the AML Compliance Officer.

Where a match to a listed entity or individual is confirmed, or where there is reasonable suspicion that a party is acting on behalf of a listed person, the Company will immediately freeze the property involved (if applicable), refrain from conducting the transaction, and report the incident to the appropriate Canadian authorities in accordance with the **Justice for Victims of Corrupt Foreign Officials Act (JVCFOA)** and applicable sanctions regulations.

The sanctions compliance framework is reviewed regularly to ensure alignment with updates issued by Canadian authorities and international sanctions bodies. Employees are trained to understand their obligations with respect to sanctions risk and reporting procedures.

9. Employee Training

NEXT SOLUTIONS CORP. provides regular training to all employees, contractors, and relevant personnel to ensure awareness and understanding of anti-money laundering (AML) and anti-terrorist financing (ATF) obligations. Training is an essential part of the Company's compliance culture and is delivered in line with the requirements of the **PCMLTFA** and **FINTRAC guidance**.

All employees must complete **mandatory AML training at least once per year**. New employees receive onboarding training as part of their induction process before being granted access to client-facing or sensitive systems. Additional training may be provided at any time in response to changes in legislation, regulatory guidance, or internal policy.

The training program covers key areas such as the Canadian legal and regulatory AML framework, identification of suspicious activity and red flags, customer due diligence, reporting obligations (e.g., STRs, LCTRs), and internal escalation procedures. Real-world scenarios and case studies may be used to help staff recognize potential money laundering and terrorist financing typologies relevant to the Company's business model.

Training completion is monitored and documented by the **AML Compliance Officer**, who maintains a log of attendance, test results (where applicable), and periodic refreshers. Failure to complete required training may result in disciplinary action.

The effectiveness of the training program is assessed regularly, and updates are made to reflect emerging risks, regulatory developments, and feedback from internal audits or compliance reviews.

10. Internal Controls and Testing

NEXT SOLUTIONS CORP. maintains a robust system of internal controls to ensure the effective implementation and ongoing integrity of its AML/ATF compliance program. These controls are designed to detect gaps, correct deficiencies, and ensure that the Company remains in full compliance with the **PCMLTFA**, **SOR/2002-184**, and guidance from **FINTRAC**.

The AML Compliance Officer conducts **periodic internal reviews** of key elements of the compliance framework, including customer onboarding processes, transaction monitoring, record-keeping practices, and the timeliness and accuracy of regulatory reporting. These reviews help identify areas for improvement and verify that day-to-day operations align with the Company's risk profile and AML obligations.

In addition to internal checks, the Company engages an **external independent reviewer at least once every two years**, as required by Canadian regulations. The scope of the review includes an evaluation of the overall design and effectiveness of the AML program, and may also involve sampling of client files, transaction reports, and staff interviews to assess operational readiness.

All findings from internal and external reviews are documented, along with a clear plan of **corrective actions** and timeframes for remediation. The Compliance Officer is responsible for implementing and tracking all remediation measures, and for reporting progress to senior management and, if applicable, the board of directors.

These periodic assessments provide an objective view of the program's health and ensure that the Company can demonstrate its commitment to regulatory compliance during regulatory inspections or enforcement reviews.

11. Incident Response and Escalation

NEXT SOLUTIONS CORP. maintains clear internal procedures for the identification, escalation, and resolution of suspicious activities or potential breaches of its AML/ATF compliance obligations. Prompt detection and proper handling of such incidents is essential for maintaining regulatory compliance and mitigating risk.

All employees are required to promptly report any activity they suspect may involve money laundering, terrorist financing, sanctions evasion, or any other financial crime. Suspicious behavior may include unusual transaction patterns, client reluctance to provide identification, use of intermediaries without clear business rationale, or transactions inconsistent with a client's known profile.

Reports of suspicious activity must be directed to the **AML Compliance Officer**. Upon receipt, the Officer will conduct an independent and documented investigation into the incident. This may include reviewing

account activity, obtaining clarification from client-facing personnel, and consulting transaction records or external data sources.

If, after reasonable assessment, the Officer determines that there are grounds to suspect a connection to a money laundering or terrorist financing offence, a **Suspicious Transaction Report (STR)** will be prepared and submitted to **FINTRAC** in accordance with applicable deadlines. The Officer is responsible for ensuring the report is complete, accurate, and filed securely.

All incidents, whether or not they result in a report to FINTRAC, are logged in the Company's **internal compliance incident register**. This register includes the nature of the suspicion, the steps taken in response, outcomes, and any remediation or policy adjustments made as a result of the case. Recurrent themes or systemic issues are escalated to senior management for further review and potential program updates.

Confidentiality is strictly maintained throughout the process, and staff are prohibited from disclosing the existence of a report to any third party, including the client involved, as per Canadian law.

12. Privacy and Data Protection

NEXT SOLUTIONS CORP. is committed to protecting the privacy and confidentiality of all personal and transactional information collected in connection with its AML/ATF obligations. The Company handles all data in compliance with the **Personal Information Protection and Electronic Documents Act (PIPEDA)** and its own internal privacy policies and procedures.

Client and transaction data is collected solely for the purposes of regulatory compliance, including client identification, transaction monitoring, and reporting obligations under the PCMLTFA. Information collected may include personal details, financial data, documentation for verification, and internal assessments or classifications related to risk.

Access to such data is strictly limited to **authorized personnel** on a need-to-know basis. The Company enforces technical and organizational safeguards to prevent unauthorized access, loss, alteration, or disclosure of sensitive information. These safeguards include secure data storage systems, user access controls, audit logs, and encryption where appropriate.

Personal data is retained only for as long as necessary to fulfill regulatory requirements, after which it is securely destroyed or anonymized in accordance with the Company's data retention and destruction policy.

Clients may request access to their personal data, subject to legal limitations, and any such requests are handled in a timely and transparent manner under the supervision of the Compliance Officer or designated privacy officer.

13. Review and Update

This Policy is reviewed **annually**, or earlier if regulatory or business changes occur. Updates are approved by the Board of Directors and implemented by the AML Officer.

Approved by:
Vladimir Kochenov
President & AML Compliance Officer
NEXT SOLUTIONS CORP.