Strategic Crypto Reserve

Know-Your-Customer (KYC) & Anti-Money Laundering (AML) Policy
(Last Updated: [Sept,23/2025])

---

1. Purpose

This Policy sets out the framework by which **Strategic Crypto Reserve ("SCR TOKEN")** conducts **Know-Your-Customer (KYC)** and **Anti-Money Laundering (AML)** procedures. The objectives are to:

- Ensure compliance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**, applicable regulations, and guidance from the **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)**.
- Protect the Company from being used to facilitate money laundering, terrorist financing, fraud, or other illicit activities.
- Safeguard customer assets and maintain trust in our platform.

---

2. Scope

This Policy applies to:

- All customers, both individuals and entities, onboarding or transacting with the Company.
- All Company personnel, contractors, and affiliates who interact with customer data, accounts, or transactions.
- All products, services, and transactions offered through **www.strategiccryptoreserve.ca**.

---

3. Customer Due Diligence (CDD)

3.1 Individual Customers

The Company shall obtain and verify:

- Full legal name
- Date of birth
- Residential address
- Government-issued identification (passport, driver's licence, national ID)

- Liveness check or selfie verification
- Contact details (email and phone)
- Occupation and source of funds/wealth
- Purpose and intended nature of the business relationship

3.2 Corporate / Institutional Customers

The Company shall obtain and verify:

- Registered legal name and incorporation details
- Jurisdiction of registration
- Certificate of incorporation / equivalent
- Articles of incorporation, bylaws, and organizational chart
- Identification of **Ultimate Beneficial Owners (UBOs)** holding 25% or more ownership
- Identity verification of directors and controlling persons
- Source of funds/wealth and business activities
- Confirmation of authority of signatories

---

4. Enhanced Due Diligence (EDD)

The Company will apply EDD measures in circumstances including, but not limited to:

- Customers from high-risk jurisdictions
- Politically Exposed Persons (PEPs) or their close associates/family members
- Complex or unusually large transactions
- Adverse media or suspicious patterns

EDD measures may include:

- Additional verification of identity and address
- Independent confirmation of information through third-party sources
- Detailed assessment of source of funds/wealth
- Senior management approval before account activation

---

5. Sanctions & Screening

- All customers are screened against Canadian, U.S., UN, EU, and other applicable **sanctions and watchlists** at onboarding and on a recurring basis.
- Customers identified as sanctioned, prohibited, or presenting unacceptable risk shall be declined or offboarded immediately.
- Screening also includes politically exposed persons (PEPs) and adverse media checks.

---

6. Ongoing Monitoring

- All transactions are subject to **continuous monitoring** using automated and manual controls.
- Alerts shall be generated for unusual activity, including rapid movement of funds, layering attempts, or deviations from the customer's stated profile.
- Transactions meeting reporting thresholds or suspicious activity indicators will be reported to **FINTRAC** in accordance with the PCMLTFA.
- Customer records shall be reviewed periodically (12–36 months, depending on risk).

---

7. Recordkeeping & Retention

- KYC and CDD records shall be maintained for a minimum of **five (5) years** after termination of the business relationship.
- Records shall be stored securely, encrypted, and accessible only to authorized personnel.
- The Company shall maintain logs of all verification checks, screening results, and risk assessments for regulatory inspection.

---

8. Roles & Responsibilities

- The Company shall appoint a **Compliance Officer / MLRO (Money Laundering Reporting Officer)**, responsible for oversight of this Policy, regulatory reporting, and staff training.
- The Compliance Officer shall escalate high-risk cases to senior management for decision-making.
- Employees are required to report any suspicions or anomalies immediately to the Compliance Officer.

---

9. Training & AwarenStrategic Crypto Reserve

Know-Your-Customer (KYC) & Anti-Money Laundering (AML) Policy

(Last Updated: [Sept, 23/2025)

1. Purpose

This Policy sets out the framework by which Strategic Crypto Reserve (“the Company”) conducts Know-Your-Customer (KYC) and Anti-Money Laundering (AML) procedures. The objectives are to:

Ensure compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), applicable regulations, and guidance from the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

Protect the Company from being used to facilitate money laundering, terrorist financing, fraud, or other illicit activities.

Safeguard customer assets and maintain trust in our platform.

2. Scope

This Policy applies to:

All customers, both individuals and entities, onboarding or transacting with the Company.

All Company personnel, contractors, and affiliates who interact with customer data, accounts, or transactions.

All products, services, and transactions offered through www.strategiccryptoreserve.ca

.

3. Customer Due Diligence (CDD)

3.1 Individual Customers

The Company shall obtain and verify:

Full legal name

Date of birth

Residential address

Government-issued identification (passport, driver's licence, national ID)

Liveness check or selfie verification

Contact details (email and phone)

Occupation and source of funds/wealth

Purpose and intended nature of the business relationship

3.2 Corporate / Institutional Customers

The Company shall obtain and verify:

Registered legal name and incorporation details

Jurisdiction of registration

Certificate of incorporation / equivalent

Articles of incorporation, bylaws, and organizational chart

Identification of Ultimate Beneficial Owners (UBOs) holding 25% or more ownership

Identity verification of directors and controlling persons

Source of funds/wealth and business activities

Confirmation of authority of signatories

4. Enhanced Due Diligence (EDD)

The Company will apply EDD measures in circumstances including, but not limited to:

Customers from high-risk jurisdictions

Politically Exposed Persons (PEPs) or their close associates/family members

Complex or unusually large transactions

Adverse media or suspicious patterns

EDD measures may include:

Additional verification of identity and address

Independent confirmation of information through third-party sources

Detailed assessment of source of funds/wealth

Senior management approval before account activation

5. Sanctions & Screening

All customers are screened against Canadian, U.S., UN, EU, and other applicable sanctions and watchlists at onboarding and on a recurring basis.

Customers identified as sanctioned, prohibited, or presenting unacceptable risk shall be declined or offboarded immediately.

Screening also includes politically exposed persons (PEPs) and adverse media checks.

6. Ongoing Monitoring

All transactions are subject to continuous monitoring using automated and manual controls.

Alerts shall be generated for unusual activity, including rapid movement of funds, layering attempts, or deviations from the customer's stated profile.

Transactions meeting reporting thresholds or suspicious activity indicators will be reported to FINTRAC in accordance with the PCMLTFA.

Customer records shall be reviewed periodically (12–36 months, depending on risk).

7. Recordkeeping & Retention

KYC and CDD records shall be maintained for a minimum of five (5) years after termination of the business relationship.

Records shall be stored securely, encrypted, and accessible only to authorized personnel.

The Company shall maintain logs of all verification checks, screening results, and risk assessments for regulatory inspection.

8. Roles & Responsibilities

The Company shall appoint a Compliance Officer / MLRO (Money Laundering Reporting Officer), responsible for oversight of this Policy, regulatory reporting, and staff training.

The Compliance Officer shall escalate high-risk cases to senior management for decision-making.

Employees are required to report any suspicions or anomalies immediately to the Compliance Officer.

9. Training & Awareness

All employees shall undergo mandatory AML/KYC training at onboarding and annually thereafter.

Training shall cover legal obligations, customer due diligence, suspicious transaction red flags, and escalation procedures.

10. Privacy & Data Protection

Customer data shall be collected and processed in compliance with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial laws.

The Company shall provide customers with clear privacy disclosures regarding data use, storage, and rights.

All personal data is encrypted in transit and at rest, and subject to strict access controls.

11. Suspicious Transaction Reporting

Employees must immediately escalate suspicious activity to the Compliance Officer.

The Compliance Officer will determine whether to file a Suspicious Transaction Report (STR) or Large Virtual Currency Transaction Report (LVCTR) with FINTRAC.

All escalations and decisions shall be documented.

12. Governance & Review

This Policy shall be reviewed annually or sooner if required by law or regulatory changes.

Updates must be approved by senior management and communicated across the Company.

Independent audits will be conducted periodically to assess effectiveness.

Approval & Adoption

This Policy has been reviewed and adopted by the Strategic Crypto Reserve on [Sept,26/2025].

- All employees shall undergo **mandatory AML/KYC training** at onboarding and annually thereafter.
- Training shall cover legal obligations, customer due diligence, suspicious transaction red flags, and escalation procedures.

---

10. Privacy & Data Protection

- Customer data shall be collected and processed in compliance with **Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)** and applicable provincial laws.
- The Company shall provide customers with clear privacy disclosures regarding data use, storage, and rights.
- All personal data is encrypted in transit and at rest, and subject to strict access controls.

---

11. Suspicious Transaction Reporting

- Employees must immediately escalate suspicious activity to the Compliance Officer.
- The Compliance Officer will determine whether to file a **Suspicious Transaction Report (STR)** or **Large Virtual Currency Transaction Report (LVCTR)** with FINTRAC.
- All escalations and decisions shall be documented.

---

12. Governance & Review

- This Policy shall be reviewed annually or sooner if required by law or regulatory changes.
- Updates must be approved by senior management and communicated across the Company.

- Independent audits will be conducted periodically to assess effectiveness.

Approval & Adoption
This Policy has been reviewed and adopted by the Board of Directors of Strategic Crypto Reserve on **2025**.