Anti-Money Laundering and Know Your Customer Policy

Last Updated: 04.09.2026

This Anti-Money Laundering and Know Your Customer Policy ("**Policy**") describes the principles and measures applied by Ostrand Ltd, a company incorporated and registered under the laws of the Republic of Seychelles under registration number 251987, having its registered office at 306 Victoria House, Victoria, Mahe, Seychelles (the "**Company**", "**we**", "**us**" or "**our**"), in connection with the prevention of money laundering, terrorist financing, sanctions evasion, fraud and other unlawful activities through B2BWALLET.

This Policy applies to the multi-currency custodial wallet service operated by the Company, together with its website, API and other interfaces through which the Service may be made available (collectively, the "**Service**").

This Policy forms part of the Company's broader framework for the responsible operation of the Service. It should be read together with the Company's Terms of Use, Privacy Policy and any other applicable rules or policies published by the Company from time to time.

The Company applies a risk-based and proportionate approach to AML, sanctions and transaction monitoring controls, taking into account the nature, functionality and risks associated with the Service.

1. Purpose And Scope

1.1. The purpose of this Policy is to establish the principles and procedures applied by the Company to:

- identify and assess risks associated with the use of the Service;
- monitor cryptocurrency Transactions for indicators of potentially unlawful or suspicious activity;
- identify potential exposure to sanctions, fraud, illicit activity and other relevant risks;
- review and investigate material compliance alerts;
- request additional information or verification where reasonably necessary;
- restrict, delay, suspend or refuse Transactions or access to the Service where appropriate;
- cooperate with competent authorities where required or permitted by applicable law; and
- maintain appropriate records relating to Transactions, compliance reviews and decisions.

1.2. This Policy applies to the Company's operation of the Service and, where relevant, to:

- Users and their Accounts;
- Transactions processed through the Service;
- Partners using the Company's API;
- blockchain addresses and other transaction-related information monitored through the Company's compliance and blockchain analytics controls; and
- any other activity conducted through or in connection with the Service that may present an AML, sanctions, fraud or other financial crime risk.

1.3. For the avoidance of doubt, where the Service is made available by a Partner to its own end customers, the Company's contractual relationship remains with the Partner in accordance with the Terms of Use. The Partner remains responsible for its own relationship with its end customers and for complying with legal or regulatory obligations applicable to its own business.
1.4. Nothing in this Policy limits the Company's right to take any action permitted under the Terms of Use or otherwise available to it under applicable law.

2. Definitions

2.1. For the purposes of this Policy:

- "**AML**" means anti-money laundering.
- "**Blockchain Analytics Provider**" means a third-party provider of blockchain analytics, transaction monitoring, wallet screening, sanctions screening or similar technology or services.
- "**CFT**" means countering the financing of terrorism.
- "**EDD**" means enhanced due diligence measures applied where the Company identifies elevated or high-risk circumstances.
- "**High-Risk Activity**" means activity which, based on the available information, presents an elevated risk of money laundering, terrorist financing, sanctions exposure, fraud, theft, cybercrime or other unlawful activity.
- "**KYC**" means know-your-customer or customer identification and verification procedures.
- "**Restricted Jurisdiction"** means a country, territory or jurisdiction in respect of which the Company has restricted or prohibited access to the Service in accordance with applicable sanctions, legal restrictions or the Company's internal risk assessment.
- "**Sanctions**" means applicable economic, financial or trade sanctions, restrictive measures, asset-freezing measures or similar restrictions imposed by competent governmental, intergovernmental or regulatory authorities.
- "**Suspicious Activity**" means activity that gives rise to reasonable concerns regarding potential money laundering, terrorist financing, sanctions violations, fraud, theft, cybercrime or other unlawful conduct.
- "**Transaction**" means an operation involving the deposit, withdrawal, transfer or conversion of digital assets through the Service.
- "**User**" has the meaning given to it in the Company's Terms of Use.

Terms not defined in this Policy have the meanings given to them in the Terms of Use, unless the context requires otherwise.

3. Governance And Responsibility

3.1. The Director of the Company is ultimately responsible for overseeing the implementation of this Policy and the Company's AML, sanctions and transaction monitoring controls.
3.2. The Director's responsibilities include, where appropriate:

- overseeing the application of this Policy;
- reviewing material AML, sanctions and compliance matters;
- determining or approving the appropriate response to elevated-risk or Suspicious Activity;

- determining whether additional information, verification or EDD should be requested;
- approving significant restrictions, suspensions or other measures where required by the circumstances;
- overseeing the maintenance of relevant compliance records; and
- reviewing and updating this Policy as appropriate.

3.3. The Company may use Blockchain Analytics Providers and other third-party service providers to support its transaction monitoring, wallet screening, sanctions-related screening and other risk management activities.

3.3.1. The Company may replace Blockchain Analytics Providers, supplement its services or engage additional providers where the Company considers this appropriate.

3.3.2. Third-party providers may generate alerts, risk indicators or other analytical information based on blockchain data and other available information. Such information may be used by the Company as part of its assessment of a Transaction or other activity.

3.3.3. The use of a third-party provider does not require the Company to treat every alert as conclusive evidence of unlawful activity. However, material alerts will be subject to an appropriate review based on the nature and severity of the identified risk.

4. Risk-Based Approach

4.1. The Company applies a risk-based approach when determining the nature and extent of monitoring, review, information requests and other compliance measures.

4.2. The level of review applied may vary depending on the circumstances of a particular Account, Transaction, blockchain address or activity.

4.3. The Company may consider one or more of the following categories of risk.

CATEGORIES OF RISK	RELEVANT FACTORS
User and Account Risk	– information provided by the User; – inaccurate, inconsistent or potentially misleading information; – unusual or suspicious use of an Account; – attempts to create or use multiple Accounts to circumvent applicable restrictions or limits; – repeated attempts to avoid or circumvent the Company's controls; – failure to provide information reasonably requested by the Company; and – other circumstances indicating elevated risk.
Transaction and Blockchain Risk	– exposure to sanctioned or potentially sanctioned blockchain addresses; – exposure to darknet marketplaces or other illicit services; – exposure to ransomware-related activity; – exposure to scams, fraud or other deceptive activity;

	– exposure to stolen, hacked or otherwise compromised digital assets; – exposure to mixers, tumblers or other services or activity intended to obscure the origin or destination of digital assets; – interactions with addresses or services identified by the Blockchain Analytics Provider as presenting elevated risk; – unusual Transaction patterns; – rapid movement of assets that appears inconsistent with the apparent purpose of the activity; – repeated or structured Transactions that appear intended to circumvent applicable limits or controls; or – any other indicators suggesting potential unlawful or Suspicious Activity.
Geographic Risk	– a User's country of residence, incorporation, nationality or place of business; – a connection between a Transaction and a Restricted Jurisdiction; – potential sanctions exposure; and – other geographic circumstances that may present an elevated financial crime or legal risk.
Partner and API Risk	Where the Service is accessed through the API, the Company may consider: – unusual or suspicious Transaction flows; – attempts to circumvent technical, transactional or compliance restrictions; – activity inconsistent with the intended use of the API; – suspected misuse of the API; and – a Partner's failure to provide information reasonably requested in connection with potentially Suspicious Activity.

5. Customer Due Diligence and KYC

5.1. The Company applies a risk-based approach to customer due diligence, identity verification and other verification measures. The scope and level of verification required may vary depending on the nature of the User, the functionality or services accessed, the characteristics of a Transaction, applicable legal or regulatory requirements, the requirements of relevant third-party service providers and the level of risk identified by the Company.

5.1.1. Accordingly, customer due diligence or KYC may not be required in the same manner or to the same extent for every User or every Transaction. However, the Company may request

information, documents or verification at any time where required by applicable law, reasonably necessary to comply with its legal or regulatory obligations, required by a relevant service provider, or appropriate in light of the risks associated with the relevant User, Account, Transaction or activity.

5.1.2. The Company may apply customer due diligence, identity verification or other review measures before granting access to certain functionality, during the use of the Service, or in connection with a particular Transaction or other activity.

5.2. **Customer Due Diligence and Verification**. Where customer due diligence or identity verification is required, the Company may request information and documents necessary to identify and verify the relevant User and to assess the nature and level of the associated risk. Depending on the circumstances, such information or documents may include:

- full legal name;
- date of birth;
- country of residence;
- contact details;
- a valid government-issued identification document;
- proof of address, where applicable;
- information regarding the purpose or intended nature of the business relationship or relevant Transaction;
- information regarding the source of funds or origin of digital assets;
- information or evidence relating to ownership or control of a relevant blockchain address or wallet; and
- any other information or documents reasonably necessary for compliance, verification or risk assessment purposes.

The scope of information and documentation requested may vary depending on whether the relevant User is an individual or a legal entity and on the nature of the relevant Service, functionality or Transaction

5.3. **Verification of Legal Entities**. Where customer due diligence or verification is required in relation to a legal entity, the Company may request information and documents including:

- the legal name of the entity;
- registration or incorporation details;
- registered address;
- information regarding directors or other persons responsible for the management of the entity;
- information regarding authorised representatives;
- information regarding beneficial owners or other persons exercising ownership or control, where applicable;
- information regarding the nature of the entity's business and intended use of the relevant functionality or Service; and
- any additional documents or information reasonably necessary for compliance, verification or risk assessment purposes.

The Company may also request identification and verification information in relation to authorised representatives, beneficial owners, directors or other relevant persons associated with the legal entity.

5.4. **Enhanced Due Diligence and Additional Review**. The Company may apply enhanced due diligence, additional verification or other enhanced review measures where a User, Account, Transaction or other activity presents an elevated level of risk. Such circumstances may include, without limitation:

- a material blockchain analytics alert;
- suspected money laundering or terrorist financing;
- sanctions concerns;
- suspected fraud, theft, cybercrime or other unlawful activity;
- a connection with a Restricted Jurisdiction;
- unusual, complex, large or unexplained Transaction activity;
- inconsistencies or concerns arising from information or documents provided by the User;
- a request or requirement from a competent authority or relevant service provider; or
- any other circumstances in which additional information or review is reasonably necessary to understand, assess or mitigate an identified risk.

5.5. Enhanced measures may include:

- requesting additional identification or verification documents;
- obtaining additional information regarding the purpose or nature of Transactions or the business relationship;
- requesting information or supporting documentation regarding the source of funds;
- requesting information or supporting documentation regarding the origin of digital assets;
- obtaining information or evidence relating to ownership or control of relevant blockchain addresses or wallets;
- conducting additional blockchain analytics or other risk analysis;
- applying enhanced or ongoing monitoring; or
- taking any other measures reasonably necessary to understand, assess or mitigate the identified risk.

5.6. **Third-Party Verification Providers**. The Company may conduct customer due diligence and verification directly and/or through third-party service providers, depending on the relevant functionality, applicable requirements and the Company's operational arrangements. Where a third-party provider is involved in providing particular functionality or conducting verification, the scope and manner of customer due diligence may also be subject to the requirements and procedures of that provider.

5.7. **Failure to Provide Required Information**. The Company may restrict, suspend, refuse to process or otherwise limit a Transaction or access to the Service or particular functionality where:

- required information or documentation is not provided;
- the Company or a relevant third-party provider is unable to complete the required verification or review;
- the information or documentation provided cannot be satisfactorily verified;
- the relevant risk cannot be adequately understood, assessed or mitigated; or
- the Company is otherwise required or permitted to take such action under applicable law, regulatory requirements or this Policy.

6. Transaction Monitoring and Blockchain Analytics

6.1. All cryptocurrency deposits processed through the Service are subject to blockchain analytics screening using the Company's Blockchain Analytics Provider. The purpose of such screening is to identify potential exposure to categories of activity that may present elevated AML, sanctions, fraud or other financial crime risks. Depending on the capabilities of the relevant Blockchain Analytics Provider, screening may identify or assess exposure to:

- sanctioned addresses or entities;
- darknet marketplaces or services;
- ransomware;
- scams and fraudulent activity;
- stolen or hacked digital assets;
- mixers, tumblers or other obfuscation services;
- terrorist financing indicators;
- high-risk or illicit services; and
- other potentially unlawful or suspicious activity identifiable through blockchain analytics.

6.2. Blockchain analytics tools may generate alerts or risk indicators in relation to a blockchain address, Transaction or other activity. The existence of an alert does not automatically establish that a User has engaged in unlawful activity. However, material alerts will be reviewed taking into account, where relevant:

- the nature and severity of the alert;
- the relevant Transaction and associated blockchain addresses;
- the available blockchain history;
- the nature and extent of the identified exposure;
- available information regarding the User or Account;
- information provided by the User or Partner, where applicable; and
- any other relevant circumstances.

The Company may take immediate precautionary measures where the nature or severity of the identified risk reasonably requires such action.

7. Alert Review, Investigation and Escalation

7.1. Potentially Suspicious Activity may be identified through:

- blockchain analytics screening;
- transaction monitoring;
- information provided by a User or Partner;
- information received from a third-party provider;
- a request, notice or other communication from a competent authority; or
- any other information available to the Company.

7.2. Where a material alert or other risk indicator is identified, the Company may conduct an initial review of the available information. The review may consider:

- the relevant Transaction;
- associated blockchain addresses;
- the type of alert or risk indicator;
- the apparent severity of the risk;
- the available blockchain history;

- the User's or Partner's previous activity, where relevant; and
- any other information reasonably available to the Company.

7.3. Where the available information is insufficient to understand or assess the identified risk, the Company may request additional information or documents. Depending on the circumstances, this may include:

- an explanation of the relevant Transaction;
- information regarding the purpose of the activity;
- source of funds information;
- information regarding the origin of digital assets;
- identification or verification information;
- evidence of ownership or control of a relevant wallet or blockchain address; or
- other information reasonably necessary for the Company's review.

The Company may delay, restrict or suspend relevant functionality while such information is being reviewed.

7.4. Following a review, the Company may determine that no further action is required or may take one or more of the following measures:

- allow or continue processing the relevant Transaction;
- continue or apply enhanced monitoring;
- request additional information or documentation;
- delay the processing of a Transaction;
- restrict specific functionality;
- suspend an Account;
- reject or refuse to process a Transaction;
- terminate a User's or Partner's access to the Service;
- preserve relevant records;
- cooperate with or provide information to a competent authority where required or permitted by applicable law; or
- take any other measure reasonably necessary to manage the identified risk or protect the Company, the Service, Users or third parties.

7.4.1. The Company is not required to process or complete a Transaction where the Company reasonably considers that doing so may expose the Company, the Service or other parties to unacceptable legal, sanctions, financial crime, fraud or security risk.

7.5. Material or elevated-risk compliance matters may be escalated to the Director for review and decision. The Director may determine the appropriate action based on the available information, the nature of the identified risk and the circumstances of the particular case.

8. Enhanced Due Diligence

8.1. The Company may apply EDD where a User, Account, Transaction or other activity presents elevated or high risk. EDD may be applied, including but not limited to, where there is:

- material exposure to high-risk or potentially illicit blockchain activity;
- potential sanctions exposure;
- a significant or unexplained blockchain analytics alert;
- Suspicious Activity;

- a connection with a Restricted Jurisdiction;
- unusual or unexplained Transaction activity;
- suspected attempts to circumvent the Company's controls; or
- another material compliance concern.
- EDD measures may include one or more of the following:
- obtaining additional information or documentation;
- requesting identification or verification information;
- requesting information regarding the source of funds;
- requesting information regarding the origin of digital assets;
- requesting an explanation of the purpose of relevant Transactions;
- conducting additional blockchain analytics or other review;
- applying enhanced monitoring; and
- delaying, restricting or suspending relevant activity pending completion of the review.

8.2. The nature and extent of EDD will depend on the circumstances and identified level of risk.

9. Sanctions and Restricted Jurisdictions

9.1. The Company seeks to identify and manage potential sanctions exposure associated with the use of the Service.

9.2. The Company's sanctions-related controls may include blockchain analytics screening, review of relevant alerts, restrictions relating to certain jurisdictions and other measures appropriate to the nature and circumstances of the identified risk.

9.3. Where the Company identifies potential sanctions exposure, it may take appropriate measures, including delaying or refusing a Transaction, restricting an Account or Service functionality, requesting additional information or cooperating with competent authorities where required or permitted by applicable law.

9.4. The Company may restrict or prohibit access to the Service from certain jurisdictions based on applicable sanctions, legal restrictions or the Company's internal risk assessment.

9.5. A connection with a Restricted Jurisdiction does not necessarily require the Company to take the same action in every case. The nature of any restriction may depend on whether the relevant jurisdiction is classified by the Company as prohibited or restricted and on the circumstances of the relevant User or activity.

9.6. The Company may request additional information or apply enhanced review where it identifies a connection with a Restricted Jurisdiction.

10. Suspicious Activity and Restrictions

10.1. The Company may take precautionary or restrictive measures where it reasonably identifies Suspicious Activity or another material compliance concern. Such measures may include:

- delaying a Transaction;
- requesting additional information;
- restricting specific functionality;
- suspending access to an Account;
- refusing to process a Transaction;

- terminating access to the Service; or
- taking other measures reasonably necessary to investigate or mitigate the identified risk.

10.2. The Company may take such measures before completing a review where immediate action is reasonably necessary due to the nature or severity of the identified risk.

10.3. Any action taken will be based on the circumstances reasonably known to the Company at the relevant time.

11. Cooperation with Competent Authorities

11.1. The Company may cooperate with law enforcement agencies, regulators and other competent authorities to the extent required or permitted by applicable law.

11.2. Upon receipt of a valid request, order or other lawful requirement, the Company may:

- preserve relevant records and information;
- provide information relating to a User, Account or Transaction;
- restrict or suspend access to the Service;
- delay, reject or otherwise restrict a Transaction;
- take measures in relation to digital assets where required or permitted by applicable law; and
- take other appropriate action in response to the relevant request or requirement.

11.3. The Company may also take appropriate action where reasonably necessary to prevent, investigate or mitigate suspected money laundering, terrorist financing, sanctions violations, fraud or other unlawful activity.

12. Confidentiality of Compliance Reviews

12.1. Information relating to internal compliance reviews, investigations, alerts and related decisions will be treated as confidential, subject to disclosure where required or permitted by applicable law or reasonably necessary for the operation of the Company's compliance controls.

12.2. The Company may be unable to disclose information concerning a compliance review, investigation or request from a competent authority where disclosure would be inappropriate or prohibited by applicable law.

13. Record Keeping

13.1. The Company will maintain records relating to Transactions and relevant compliance activities for a period of **five (5) years**, unless a longer retention period is required or permitted by applicable law or is reasonably necessary in connection with an ongoing investigation, dispute or request from a competent authority. Records may include, where applicable:

13.2. Transaction records;

- blockchain addresses and transaction identifiers;
- blockchain analytics and screening results;
- compliance alerts and risk indicators;
- information and documents obtained from Users or Partners;
- records of requests for additional information;
- EDD information;

- records of material reviews and investigations;
- decisions and measures taken by the Company; and
- relevant communications with competent authorities.

13.3. Records may be maintained in electronic form and should, where applicable, enable the Company to demonstrate the basis upon which a material compliance decision was taken.

14. Review and Updates

14.1. The Director will review this Policy periodically and may update it where appropriate.

14.2. This Policy may be reviewed or amended in particular where:

- the functionality or nature of the Service changes;
- the Company changes or introduces Blockchain Analytics Providers or other relevant service providers;
- new or materially different risks are identified;
- applicable legal or sanctions requirements change; or
- the Company otherwise considers an update necessary or appropriate.

14.3. The Company may amend this Policy from time to time by publishing an updated version through the Website or otherwise making it available through the Service.

15. Contact Information

15.1. For questions relating to this Policy or the Company's compliance procedures, Users may contact the Company at support@b2bwallet.io.

ANNEX 1. RESTRICTED JURISDICTIONS

The Company applies a risk-based approach to jurisdictional risk and may restrict or prohibit access to the Service in relation to certain countries, territories or jurisdictions based on applicable sanctions, legal and regulatory requirements, AML/CFT risks and the Company's internal risk assessment.

The Company does not maintain an exhaustive list of prohibited or restricted jurisdictions in this AML Policy. The applicable restrictions may be determined and updated from time to time based on relevant sanctions lists, applicable legal requirements, FATF publications and the Company's internal risk assessment.

Users located in, resident in, incorporated or otherwise connected with jurisdictions subject to applicable sanctions, significant AML/CFT risks or other legal or regulatory restrictions may be prohibited from accessing or using the Service, or may be subject to additional review, enhanced monitoring, requests for information, transaction restrictions or other risk-based measures.

The Company may also apply restrictions where a User, wallet address, transaction, transaction counterparty or other relevant activity is directly or indirectly connected with a jurisdiction presenting elevated sanctions, AML/CFT or other compliance risks.

The fact that a User is connected with a particular jurisdiction does not, by itself, necessarily result in the refusal of access to the Service, unless such restriction is required by applicable law, sanctions or the Company's internal risk assessment.

The Company may update its jurisdictional restrictions from time to time without amending this AML Policy, provided that such restrictions remain consistent with applicable law and the Company's internal risk assessment.

ANNEX 2. COMPLIANCE REVIEW REPORT

Case Reference: _____
Date Opened: _____
Date Closed: _____

1. SUBJECT OF REVIEW

User / Account: _____
Partner, if applicable: _____
Transaction ID(s): _____
Relevant Blockchain Address(es): _____
Digital Asset: _____
Amount: _____

2. ALERT OR RISK INDICATOR

Alert Source:

☐ Blockchain Analytics Provider: _____
☐ Internal Monitoring
☐ Partner Information
☐ Competent Authority Request
☐ Other:
_____
_____

Alert / Risk Category:

☐ Sanctions Exposure
☐ Darknet Exposure
☐ Ransomware
☐ Fraud / Scam
☐ Stolen or Hacked Assets
☐ Mixer / Obfuscation Service
☐ Suspicious Transaction Pattern
☐ Restricted Jurisdiction
☐ Other:
_____
_____

Risk Level:

☐ Low
☐ Medium

☐ High

Summary of Alert or Risk Indicator:

_____

_____

_____

3. INFORMATION REVIEWED

☐ Transaction Details
☐ Blockchain Analytics Results
☐ Blockchain Address History
☐ Account Information
☐ Information Provided by User
☐ Information Provided by Partner
☐ Source of Funds Information
☐ Additional Documents
☐ Other:

_____

_____

Summary of Information Reviewed:

_____

_____

_____

4. ADDITIONAL INFORMATION REQUESTED

☐ No Additional Information Requested
☐ Transaction Explanation
☐ Identification Information
☐ Source of Funds
☐ Origin of Digital Assets
☐ Proof of Wallet Ownership or Control
☐ Other:

_____

_____

Summary / Outcome:

_____

_____

_____

5. FINDINGS

Summary of Review and Findings:

_____

_____

_____

6. DECISION

☐ No Further Action Required

☐ Transaction Allowed / Continued

☐ Enhanced Monitoring Applied

☐ Additional Information Requested

☐ Transaction Delayed

☐ Transaction Rejected

☐ Functionality Restricted

☐ Account Suspended

☐ Access Terminated

☐ Records Preserved

☐ Cooperation with Competent Authority Required

☐ Other Action:

_____

_____

Reasoning for Decision:

_____

_____

_____

7. DIRECTOR REVIEW

Reviewed / Approved by:

Name: _____

Position: Director

Date: _____

Signature / Approval Record: _____