1. Purpose and Scope

1.1 **Purpose.**
This *Know Your Customer (KYC) and Anti–Money Laundering (AML) Policy* ("**Policy**") establishes the internal framework and operational standards of **Anytime Technologies Limited**, trading as **PAY247** ("**Company**"), for the prevention and detection of money laundering, terrorist financing, fraud, and related financial crimes. The Policy is designed to ensure full compliance with the **BVI Anti–Money Laundering Regulations, 2008**, the **Anti–Money Laundering and Terrorist Financing Code of Practice, 2008**, and the **Financial Investigation Agency Act, 2003**, as amended from time to time.

1.2 **Scope.**
This Policy applies to all officers, employees, contractors, representatives, and affiliates of the Company, and governs all relationships with **Customers**, **Merchants**, **End Users**, and any other counterparties who use or access PAY247's products or services. It applies to all business units, regardless of geographic location, and covers all transactions conducted in connection with PAY247's operations, including payment processing, payouts, settlements, and related financial activities.

1.3 **Objectives.**
The objectives of this Policy are to:
(a) establish a robust framework for identifying, verifying, and monitoring customers and transactions;
(b) ensure that PAY247 does not knowingly or negligently facilitate money laundering, terrorist financing, or any other financial crime;
(c) maintain adequate systems, controls, and procedures consistent with BVI laws and internationally accepted standards such as the **Financial Action Task Force (FATF)** Recommendations; and
(d) promote a culture of compliance and ethical conduct across all levels of the Company.

1.4 **Legal and Regulatory Alignment.**
This Policy is interpreted in conjunction with:

- The Anti–Money Laundering Regulations, 2008 (BVI);
- The Anti–Money Laundering and Terrorist Financing Code of Practice, 2008 (BVI);
- The Financial Investigation Agency Act, 2003;
- Applicable guidance notes issued by the BVI Financial Services Commission and Financial Investigation Agency (FIA); and
- International AML/CFT standards including FATF and the Wolfsberg Principles.

1.5 **Continuous Improvement.**
The Company will periodically review and update this Policy to reflect changes in legislation,

regulatory expectations, or the Company's business model, ensuring its adequacy and effectiveness remain current.

2. Definitions and Interpretations

2.1 **Definitions.**
For purposes of this Policy, unless the context otherwise requires:

- **"AML/CFT"** means Anti–Money Laundering and Countering the Financing of Terrorism.
- **"Beneficial Owner"** means a natural person who ultimately owns or controls a Customer or the person on whose behalf a transaction is being conducted.
- **"Customer Due Diligence (CDD)"** refers to the process of identifying and verifying the identity of a Customer and understanding the purpose and intended nature of the business relationship.
- **"Enhanced Due Diligence (EDD)"** means additional due diligence measures applied to higher-risk customers or transactions.
- **"Financial Investigation Agency (FIA)"** refers to the statutory agency established under the FIA Act responsible for receiving and investigating suspicious activity reports in the BVI.
- **"Merchant"** means a business customer who uses PAY247's payment gateway or payout services to receive or send payments.
- **"End User"** means an individual or entity making or receiving payments through PAY247's systems, other than the Merchant.
- **"Money Laundering"** has the meaning assigned by the **Proceeds of Criminal Conduct Act, 1997 (as amended)**, and includes the process of concealing, disguising, converting, transferring, or removing criminal property.
- **"Politically Exposed Person (PEP)"** means an individual who is or has been entrusted with a prominent public function, including family members or close associates thereof.
- **"Suspicious Activity Report (SAR)"** means a report filed with the FIA detailing any knowledge, suspicion, or reasonable grounds for suspicion of money laundering or terrorist financing.
- **"Transaction Monitoring"** means the review of financial transactions to detect unusual patterns, anomalies, or activities inconsistent with the Customer's known profile.

2.2 **Interpretation.**
References to "the Company" include PAY247 and all its controlled entities. Terms not expressly defined herein shall bear the meaning assigned under BVI law. In the event of conflict between this Policy and local regulations, the stricter standard shall apply.

2.3 **Integration with Other Policies.**
This Policy should be read alongside the Company's **Privacy Policy**, **Terms and Conditions**, and **Data Security Policy**, all of which collectively govern how customer data is collected, processed, and safeguarded.

3. Governance and Responsibility

3.1 **Compliance Oversight.**
The Company shall designate a suitably qualified **Money Laundering Reporting Officer (MLRO)** who shall be responsible for oversight and administration of the Company's AML/CFT framework. The MLRO shall have direct access to senior management and the authority to:
(a) receive and investigate internal reports of suspicious activity;
(b) determine whether a Suspicious Activity Report (SAR) should be submitted to the FIA;
(c) maintain records of investigations, decisions, and communications; and
(d) liaise with the FIA, law enforcement agencies, and regulators.

3.2 **Deputy MLRO.**
A **Deputy MLRO** may be appointed to act in the absence of the MLRO and to support operational compliance functions. The Deputy MLRO shall possess appropriate knowledge, independence, and authority to carry out such duties.

3.3 **Senior Management Responsibility.**
The Board of Directors and senior management are ultimately accountable for ensuring effective implementation of this Policy. They shall:
(a) approve and periodically review the AML/CFT framework;
(b) allocate adequate resources and staffing to maintain compliance;
(c) promote awareness and training throughout the organization; and
(d) ensure that compliance is embedded within the Company's risk management and governance processes.

3.4 **Employee Responsibilities.**
All employees and agents must adhere to this Policy and promptly report any knowledge or suspicion of money laundering, terrorist financing, or other suspicious activity to the MLRO. Employees are prohibited from disclosing or "tipping off" any person who is the subject of an internal or external report.

3.5 **Independence and Authority.**
The MLRO shall operate independently of commercial departments and may escalate issues directly to the Board. No person shall obstruct, influence, or retaliate against the MLRO or any employee for fulfilling obligations under this Policy or applicable law.

3.6 **Accountability Statement.**
The Company affirms its full commitment to maintaining a culture of compliance, transparency, and zero tolerance toward financial crime. Any breach of this Policy may result in disciplinary action, including termination and referral to competent authorities.

3.7 Outsourcing. Where AML/CFT activities (including KYC, screening, monitoring, case management, or archival) are outsourced to third parties, the Company shall (a) conduct due diligence on the service provider; (b) maintain a written agreement allocating responsibilities and audit rights; (c) test the provider at least annually; and (d) remain fully responsible for compliance outcomes.

3.8 Reliance on Third Parties. The Company may rely on regulated third parties to perform CDD only where permitted by BVI law and subject to written assurances that underlying identification data and documents will be provided promptly upon request. Reliance shall not limit the Company's liability for AML/CFT compliance.

3.9 Employee Due Diligence. Pre-employment screening (including identity, right-to-work, criminal record checks where lawful, and employment references) is required for personnel in sensitive roles. Screening shall be refreshed proportionate to risk.

4. Risk-Based Approach

4.1 **Principle.**
The Company adopts a *risk-based approach (RBA)* to anti-money laundering and counter-terrorist financing, meaning that the intensity of due diligence, monitoring, and control measures shall be proportionate to the level of risk presented by each customer, product, service, or transaction.

4.2 **Risk Assessment Framework.**
The Company conducts periodic enterprise-level risk assessments that evaluate exposure across the following dimensions:
(a) **Customer Risk** – nature, type, and behaviour of customers (e.g., merchants, individual users, or intermediaries);
(b) **Geographical Risk** – countries of incorporation, residence, or transaction origination;
(c) **Product and Service Risk** – types of payment or payout services offered;
(d) **Delivery Channel Risk** – non-face-to-face onboarding, cross-border activities, and digital KYC methods; and
(e) **Transactional Risk** – volume, frequency, or complexity inconsistent with expected usage.
(i) cash deposits, anonymous instruments, or bearer-form payment products;
(ii) transactions where the true originator or beneficiary cannot be reasonably identified and verified.

4.3 **Risk Rating.**
Each customer shall be assigned a risk classification (low, medium, or high). This classification determines the level of due diligence and ongoing monitoring required. High-risk customers shall not be onboarded or maintained without MLRO approval.

4.4 **Periodic Review.**
The risk assessment shall be reviewed annually, or sooner if material changes occur in the Company's business model, product suite, or regulatory environment. The MLRO shall document all changes and ensure resulting control enhancements are implemented promptly.

4.5 **Prohibited and Restricted Relationships.**
The Company will not establish or maintain business relationships with:
(a) anonymous or fictitious accounts;
(b) shell banks or unregulated payment intermediaries;
(c) customers located in or associated with jurisdictions subject to FATF sanctions or BVI

prohibitions; or
(d) entities or individuals appearing on applicable sanctions lists.

5. Customer Due Diligence (CDD)

5.1 **General Obligation.**
Before establishing any business relationship or processing any transaction, the Company shall conduct adequate due diligence to identify and verify the identity of the Customer and, where applicable, its Beneficial Owners.

5.2 **Individual Customers.**
For individual End Users, CDD shall include collection and verification of:
(a) full legal name;
(b) date of birth;
(c) residential address;
(d) nationality;
(e) government-issued identification number and document copy; and
(f) source of funds and, where relevant, source of wealth.

5.3 **Corporate Customers / Merchants.**
For merchants or other legal entities, the Company shall obtain and verify:
(a) legal name and registration number;
(b) incorporation certificate and constitutional documents;
(c) principal place of business and registered address;
(d) names and identification of directors and authorised signatories;
(e) identification and verification of each Beneficial Owner holding, directly or indirectly, 25% or more ownership or control; and
(f) description of the nature and purpose of the business relationship.

5.4 **Verification Procedures.**
Identity verification shall be performed using reliable, independent source documents, data, or information, which may include:
(a) government-issued identification documents;
(b) business registry extracts;
(c) bank confirmation letters or utility bills; or
(d) approved third-party electronic verification databases.

5.5 **Timing of CDD.**
Verification must be completed prior to the establishment of a business relationship or execution of any transaction. In exceptional cases where verification is delayed, it must be completed as soon as practicable and before any payout or withdrawal is permitted.

5.6 **Ongoing CDD Obligations.**
The Company shall ensure that customer information remains accurate and up-to-date throughout the relationship. Material changes to a customer's ownership, address, or risk profile must trigger re-verification.

5.7 **Failure to Complete CDD.**
If a customer fails to provide adequate identification or verification information, the Company shall not open or continue the account and shall consider filing a Suspicious Activity Report with the FIA.

5.8 Refusal to Onboard.

The Company shall decline onboarding where CDD cannot be completed to a satisfactory standard, the risk is unacceptable, or onboarding would breach sanctions or law.

5.9 Relationship Exit.

The Company may suspend or terminate a relationship where (a) CDD/EDD cannot be refreshed; (b) suspicious activity persists; or (c) continued service would contravene law or policy.

6. Enhanced and Simplified Due Diligence

6.1 **Enhanced Due Diligence (EDD).**
EDD shall be applied where the customer or transaction presents a higher-than-normal risk, including but not limited to:
(a) politically exposed persons (PEPs) or their close associates;
(b) customers from or transactions involving high-risk jurisdictions identified by FATF or the BVI authorities;
(c) complex ownership or trust structures;
(d) unusually large or opaque transactions inconsistent with expected activity; and
(e) cross-border payments lacking clear economic rationale.

6.2 **EDD Measures.**
EDD measures may include:
(a) obtaining additional information on the customer's identity, ownership, and business operations;
(b) verifying the source of funds and source of wealth;
(c) obtaining senior management approval before establishing or continuing the relationship; and
(d) increasing the frequency and intensity of transaction monitoring and review.

6.3 **Simplified Due Diligence (SDD).**
Where the risk of money laundering or terrorist financing is demonstrably low and where permitted by BVI law, the Company may apply simplified measures. SDD is limited to customers such as:
(a) licensed financial institutions regulated under equivalent AML/CFT standards;
(b) publicly listed companies with securities traded on recognised stock exchanges; and
(c) government entities or agencies.

6.4 **Restrictions on SDD.**
SDD shall not apply where there is suspicion of money laundering, terrorist financing, or where the customer or transaction involves a high-risk jurisdiction.

6.5 **Documentation and Approval.**
All EDD and SDD determinations must be documented, justified, and approved by the MLRO or a delegated senior compliance officer.

7. Ongoing Monitoring

7.1 **Purpose of Monitoring.**
Ongoing monitoring enables the Company to detect and respond to suspicious, unusual, or inconsistent customer behaviour during the course of the business relationship. It ensures that transactions remain consistent with the Customer's known profile, stated business activities, and declared source of funds.

7.2 **Monitoring Methods.**
The Company employs both automated and manual processes to identify anomalies. Monitoring shall include:
(a) real-time screening of transactions against internal risk thresholds;
(b) daily batch reviews of transaction patterns for unusual activity; and
(c) periodic account reviews proportionate to the customer's risk rating.

7.3 **Key Monitoring Indicators.**
Indicators triggering review may include, but are not limited to:

- multiple small payments structured to avoid thresholds;
- significant changes in transaction frequency or size;
- unexplained cross-border transfers;
- use of third-party or proxy accounts; or
- transactions inconsistent with the stated nature of business.

7.4 **Periodic Review.**
High-risk customers shall be subject to enhanced monitoring and quarterly reviews. Medium-risk customers will be reviewed annually, and low-risk customers biennially, unless material changes arise.

7.5 **Review Outcomes.**
Monitoring results shall be documented and retained as part of the compliance record. The MLRO shall review flagged activity and determine whether escalation or filing of a Suspicious Activity Report (SAR) is warranted.

8. Politically Exposed Persons (PEPs) and Sanctions Screening

8.1 **Definition and Identification.**
A Politically Exposed Person (PEP) includes any individual who is or has been entrusted with a prominent public function, whether domestic or foreign, as well as their immediate family members and known close associates.

8.2 **Screening Process.**
The Company screens all new and existing customers, beneficial owners, and related parties against:
(a) global PEP databases;
(b) international sanctions lists, including the United Nations, European Union, Office of Foreign Assets Control (OFAC), and BVI-issued lists; and
(c) adverse media and law enforcement watchlists.

8.3 **Onboarding and Approval.**
Where a customer is identified as a PEP or linked to a sanctioned person or jurisdiction:
(a) onboarding or continuation of the relationship shall require prior written approval of the MLRO and senior management;
(b) enhanced due diligence must be performed to establish the legitimacy of source of funds and source of wealth; and
(c) transactions involving PEPs shall be subject to heightened monitoring and periodic review.

8.4 **Prohibited Relationships.**
The Company will not engage in any transaction or relationship involving:
(a) individuals or entities subject to comprehensive sanctions;
(b) shell banks; or
(c) any person or jurisdiction where doing so would contravene BVI or international AML/CFT restrictions.

8.5 **Ongoing Screening.**
Customer databases shall be continuously screened against updated sanctions and PEP lists. Any match or potential match shall be reviewed promptly by the MLRO for verification and escalation.

8.6 Cadence.
Screening shall occur (a) prior to onboarding; (b) daily against refreshed sanctions/PEP lists; and (c) upon material changes to customer profiles.

8.7 Sources.
Screening lists shall include, at a minimum, UN, EU, OFAC, and BVI lists, plus reputable adverse-media datasets; list updates shall be ingested within 24 hours of publication.

9. Suspicious Activity Detection and Reporting

9.1 **Identification of Suspicious Activity.**
Suspicious activity may include unusual patterns, inconsistent behaviour, or transactions lacking clear economic or lawful purpose. Examples include:
(a) rapid movement of funds through multiple accounts without business justification;
(b) mismatched names between sender and account holder;
(c) large transfers from or to high-risk jurisdictions; or
(d) repeated attempts to circumvent transaction thresholds or verification.

9.2 **Internal Reporting Procedures.**
(a) Employees must immediately report any suspicion or knowledge of money laundering, terrorist financing, or other criminal activity to the MLRO.
(b) Reports must be made in writing and contain all relevant facts, documents, and observations.
(c) Employees must not discuss or disclose the report or its contents to any person outside the compliance chain ("tipping-off" is strictly prohibited).

9.3 **MLRO Assessment.**
The MLRO shall:
(a) acknowledge receipt of each internal report;
(b) conduct an initial assessment to determine if a reasonable suspicion exists;
(c) document findings and maintain an internal log; and
(d) where appropriate, prepare and submit a **Suspicious Activity Report (SAR)** to the **Financial Investigation Agency (FIA)** without delay.

9.4 **Post-Reporting Obligations.**
Once a SAR is filed, the Company shall fully cooperate with the FIA or law enforcement authorities, including preserving all relevant records and refraining from transactions likely to prejudice investigations.

9.5 **Confidentiality and Protection.**
All SARs, internal reports, and related communications are confidential. Employees making reports in good faith shall not face retaliation or adverse action for compliance-related disclosures.

9.6 Whistleblowing. Employees and contractors may report concerns confidentially to the MLRO. Good-faith reporters are protected from retaliation.

10. Record-Keeping and Retention

10.1 **Legal Requirement.**
The Company shall maintain complete and accurate records in accordance with the **BVI Anti–Money Laundering Regulations** and **Code of Practice**, ensuring information is sufficient to enable reconstruction of transactions and identification of parties involved.

10.2 **Retention Period.**
(a) All customer identification and verification documents, business correspondence, and transaction records shall be retained for a **minimum period of five (5) years** following the termination of the business relationship or completion of the transaction, whichever is later.
(b) Records relating to ongoing investigations or regulatory inquiries shall be retained until the matter is formally closed, even if this extends beyond the statutory minimum.

10.3 **Storage and Security.**
(a) Records shall be stored securely in encrypted digital form with controlled access limited to authorised personnel only.
(b) Backups shall be maintained in redundant secure locations to prevent data loss or tampering.

(c) Destruction of expired records must be performed securely, ensuring data cannot be reconstructed.

10.4 **Retrievability.**
All retained records must be capable of being retrieved promptly upon request from competent authorities or the MLRO, and shall be made available within the statutory timeframe prescribed by BVI law.

10.5 **Audit Trail.**
An audit log shall be maintained for all access to or modification of compliance records, ensuring accountability and evidentiary integrity.

11. Wire Transfers and Originator Information

11.1 **Legal Obligation.**
In accordance with the **BVI Anti–Money Laundering Regulations** and the **Code of Practice**, the Company shall ensure that all wire transfers are accompanied by complete and accurate information on the **originator** (payer) and **beneficiary** (payee). This enables effective traceability and detection of illicit transactions within the financial system.

11.2 **Required Originator Information.**
Each wire transfer must include the following data elements for the originator:
(a) full name;
(b) account number or unique transaction identifier; and
(c) full residential or business address, national identity number, or date and place of birth.

11.3 **Required Beneficiary Information.**
Each wire transfer must also include:
(a) full name of the beneficiary; and
(b) account number or unique transaction reference enabling identification.

11.4 **Verification.**
The Company shall verify the accuracy of the originator's and beneficiary's details before executing the transfer. Inbound transactions lacking required information shall be subject to verification, delay, or rejection pending clarification.

11.5 **Intermediary Institutions.**
Where the Company acts as an intermediary, it must ensure that all received and outgoing transfer messages contain the complete originator and beneficiary information. The Company shall not accept or forward transfers with incomplete data unless corrective measures are taken.

11.6 **Monitoring and Reporting.**
The MLRO shall ensure ongoing monitoring of wire transfer data to identify repeated deficiencies or patterns indicative of suspicious activity. Where deficiencies cannot be resolved, a Suspicious Activity Report (SAR) shall be filed with the **Financial Investigation Agency (FIA)**.

11.7 Deficiencies.
Repeated failure by counterpart institutions to transmit complete originator/beneficiary data may result in restriction, suspension, or termination of the correspondent relationship and, where appropriate, SAR filing.

12. Independent Testing and Audit

12.1 **Purpose.**
The Company's AML/CFT framework shall be subject to periodic **independent testing** to assess the adequacy and effectiveness of its controls, procedures, and implementation.

12.2 **Frequency and Scope.**
(a) Independent testing shall occur **at least annually** or whenever significant changes occur in business operations, systems, or regulatory obligations.
(b) The audit shall evaluate:

- compliance with BVI AML laws and this Policy;
- adequacy of internal controls and record-keeping;
- transaction monitoring effectiveness; and
- staff training and awareness levels.

12.3 **Independence.**
Testing shall be conducted by personnel independent of the operational and compliance functions, or by qualified external auditors engaged for that purpose.

12.4 **Reporting.**
Findings of each review shall be documented in a formal report delivered to the **Board of Directors** and the **MLRO**, detailing identified deficiencies, recommendations, and required remedial actions.

12.5 **Corrective Actions.**
Management must address all audit findings within agreed timelines, document remediation steps, and ensure closure is verified through follow-up testing.

13. Training and Awareness

13.1 **Mandatory Training.**
All employees, officers, and relevant contractors must complete AML/CFT training upon hire and thereafter on an **annual basis**. This training shall cover:
(a) obligations under this Policy and BVI AML laws;
(b) methods of money laundering and terrorist financing relevant to payment services;
(c) red-flag indicators of suspicious transactions;
(d) internal reporting procedures and tipping-off prohibitions; and
(e) record-keeping and confidentiality duties.

13.2 **Specialised Training.**
Employees in high-risk or compliance-sensitive roles (e.g., customer onboarding, transaction monitoring, or payouts) shall receive additional in-depth training tailored to their specific functions.

13.3 **Assessment and Certification.**
Training effectiveness shall be measured through assessments or acknowledgment of completion. Records of participation and results shall be retained for at least five (5) years.

13.4 **Awareness Culture.**
The Company fosters a culture of compliance and ethical awareness by ensuring that all personnel understand their role in preventing money laundering and financial crime. Periodic communications, workshops, and compliance updates will reinforce awareness.

14. Data Protection and Confidentiality

14.1 **Principle.**
The Company shall handle all personal data collected for AML/KYC purposes in strict compliance with applicable data protection laws, including principles of lawfulness, fairness, and transparency.

14.2 **Purpose Limitation.**
Personal data obtained for AML/CFT purposes shall be used solely for:
(a) identification and verification of customers;
(b) ongoing monitoring and risk assessment; and
(c) fulfilment of legal or regulatory obligations, including reporting to competent authorities.

14.3 **Access Control.**
Access to AML-related data shall be limited to authorised personnel who require it to perform their duties. All employees with access shall be bound by confidentiality agreements.

14.4 **Data Sharing.**
Data may be shared only with:
(a) the **Financial Investigation Agency (FIA)**, **BVI Financial Services Commission**, or other competent authorities upon lawful request;
(b) third-party service providers performing regulated AML functions under written agreement ensuring equivalent confidentiality and security standards; or
(c) financial institutions or partners, where such sharing is necessary for transaction processing and permitted by law.

14.5 **Data Retention and Deletion.**
AML/KYC data shall be retained for the minimum statutory period required under Section 10 of this Policy and securely deleted or anonymised thereafter, unless extended retention is legally required.

14.6 **Confidentiality Assurance.**
All employees are prohibited from disclosing or misusing customer information. Breach of confidentiality shall constitute gross misconduct and may result in disciplinary and legal action.

15. Policy Review and Updates

15.1 **Review Cycle.**
This Policy shall be reviewed by the **Money Laundering Reporting Officer (MLRO)** at least **annually**, or earlier if required by legislative, regulatory, or operational changes affecting the Company's AML/CFT obligations.

15.2 **Trigger Events for Interim Review.**
An extraordinary review shall be initiated in the event of:
(a) amendments to BVI AML/CFT legislation or FATF recommendations;
(b) introduction of new PAY247 products, payment methods, or markets;
(c) findings or recommendations from internal or external audits; or
(d) identification of material compliance deficiencies or enforcement actions within the industry.

15.3 **Revision Approval.**
All material amendments to this Policy must be reviewed and approved by the **Board of Directors** prior to implementation. Minor technical or procedural updates may be authorised by the MLRO, provided they are reported at the next board meeting.

15.4 **Communication of Changes.**
Once approved, any changes to the Policy shall be promptly communicated to all relevant employees, contractors, and business partners. The updated version shall be made accessible through the Company's internal compliance portal and retained in official records.

15.5 **Record of Revisions.**
A revision log shall be maintained by the MLRO, detailing the date, nature, and authorisation of each amendment, along with distribution and acknowledgment records.

16. Governing Law and Enforcement

16.1 Applicable Law.
This Policy and all compliance obligations arising under it shall be governed by and construed in accordance with the laws of the **British Virgin Islands**.

16.2 Dispute Resolution.
(a) The Company encourages the amicable resolution of any disagreement or claim arising out of or in connection with this Policy.

(b) Accordingly, any dispute between the Company and its officers, employees, contractors, or business partners that does not involve a regulatory or criminal investigation shall first be submitted to **good-faith mediation** in the British Virgin Islands.

(c) If mediation is unsuccessful within thirty (30) days of a written request for mediation, the dispute shall be finally resolved by **binding arbitration** under the **BVI International Arbitration Centre (BVI IAC)** Rules in force at the time of the dispute.

(d) The seat of arbitration shall be **Road Town, Tortola, British Virgin Islands**. The language of arbitration shall be **English**. The arbitral award shall be final and binding on the parties and may be enforced in any court of competent jurisdiction.

16.3 Regulatory and Enforcement Matters.
Nothing in this Section shall limit or delay the Company's statutory obligation to cooperate fully with competent BVI or international authorities in the prevention, investigation, or prosecution of money-laundering, terrorist-financing, or other financial crimes. For avoidance of doubt, matters involving regulatory compliance or criminal liability shall remain subject to the jurisdiction of the **courts of the British Virgin Islands**.

16.4 Non-Compliance.
Failure by any officer, employee, or contractor to comply with this Policy may result in disciplinary action up to and including termination of employment or contract, civil penalties, or criminal prosecution where applicable.

16.5 Supremacy of Law.
Where any provision of this Policy conflicts with mandatory requirements of BVI law, the legal requirement shall prevail.