ICT ZONE ASIA BERHAD
REGISTRATION NO. 201901003459 (1312785-X)

Anti-Money Laundering, Countering Financing Of Terrorism, Countering Proliferation Financing And Targeted Financial Sanctions Policy

1. PURPOSE, OBJECTIVES AND SCOPE

(a) This Policy establishes the anti-money laundering, countering financing of terrorism, countering proliferation financing and targeted financial sanctions ("AML/CFT/CPF and TFS") framework of ICT Zone Asia Berhad and its subsidiaries (collectively, the "Group").

(b) The Group is committed to conducting its businesses with integrity and in compliance with all applicable laws and regulatory requirements relating to the prevention of money laundering, terrorism financing and proliferation financing and the implementation of targeted financial sanctions.

(c) This Policy establishes the minimum principles, governance arrangements and controls to be observed throughout the Group to identify, assess, monitor, manage and mitigate money laundering, terrorism financing and proliferation financing risks ("ML/TF/PF Risks").

(d) This Policy applies to all directors, officers, employees and, where relevant, representatives or persons acting on behalf of a member of the Group.

(e) Each member of the Group shall comply with this Policy as a minimum Group standard. Where a member of the Group constitutes a "reporting institution" under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("AMLA") or is otherwise subject to specific AML/CFT/CPF or TFS requirements, that member shall additionally comply with all statutory, regulatory and supervisory requirements applicable to it. As a minimum, and in a manner proportionate to the nature, size and ML/TF/PF risk of its business, every member of the Group (whether or not it is a Reporting Institution, as defined in paragraph 1(f)) shall:

i. take reasonable measures to identify its customers and business counterparties;
ii. screen its customers and business counterparties against applicable sanctions and designation lists and comply with any freezing, blocking, prohibition or reporting obligations applicable to it;
iii. ensure that any knowledge or suspicion of ML/TF/PF is escalated internally in accordance with paragraph 7; and
iv. provide appropriate awareness training to relevant personnel and maintain appropriate records.

(f) For the purposes of this Policy, "Reporting Institution" means any member of the Group which is a reporting institution under AMLA and is subject to the AML/CFT/CPF and TFS requirements administered by Bank Negara Malaysia ("BNM"), and "SKP-Regulated Entity" means any member of the Group which is authorised by, or has applied for authorisation from, SKP (as defined in paragraph 2(a)(iii)) in respect of its leasing or other consumer credit business. The members of the Group which are Reporting Institutions and/or SKP-Regulated Entities as at the Effective Date are set out in Schedule 1. Schedule 1 may be updated by Senior Management, with notification to the Board, to reflect any change in the regulatory status of a member of

the Group, and such update shall not constitute an amendment to this Policy. Any member of the Group which is or becomes subject to specific AML/CFT/CPF or TFS regulatory requirements shall accordingly implement this Policy together with such additional procedures, systems and controls as are necessary to comply with its specific regulatory obligations.

This Policy supplements, and does not replace, the Group Anti-Bribery and Corruption Policy or any other applicable compliance, risk management, data protection or internal control policy of the Group.

(g) Where any applicable law, regulation, standard, guideline, directive or regulatory requirement imposes a higher or more stringent requirement than this Policy, the higher or more stringent requirement shall prevail.

2. REGULATORY FRAMEWORK

(a) For the purposes of this Policy, "Applicable Law" includes, to the extent applicable to the relevant member of the Group:
   i. AMLA and all subsidiary legislation, orders and requirements issued thereunder, as amended from time to time;
   ii. BNM's applicable policy documents, standards, guidelines, circulars, directives and requirements relating to AML/CFT/CPF and TFS for designated non-financial businesses and professions and non-bank financial institutions;
   iii. the Consumer Credit Act 2025, the Authorisation Standards and Conduct Standards issued by Suruhanjaya Kredit Pengguna / the Consumer Credit Commission ("SKP"), and other applicable SKP requirements;
   iv. the Strategic Trade Act 2010 and applicable legislation and regulatory requirements relating to targeted financial sanctions and proliferation financing;
   v. applicable United Nations Security Council sanctions and domestic sanctions or designation orders implemented under Malaysian law; and
   vi. any other Malaysian law or regulatory requirement applicable to the relevant member of the Group.

(b) References in this Policy to any legislation, regulatory instrument or requirement include any amendment, replacement or re-enactment thereof from time to time.

3. GOVERNANCE

(a) The Board of Directors of ICT Zone Asia Berhad shall oversee the implementation of this Policy as a Group policy. Each member of the Group which is a Reporting Institution shall remain responsible for complying with the AML/CFT/CPF and TFS obligations applicable to it, and the board of that Reporting Institution shall retain ultimate responsibility and accountability for such compliance. This Policy shall also be adopted by the board of directors of each Reporting Institution and each SKP-Regulated Entity. The relevant Board shall:

   i. approve this Policy and any material amendments thereto;
   ii. provide appropriate oversight of the relevant member of the Group's ML/TF/PF Risks;
   iii. ensure that adequate authority, resources and reporting lines are provided for the effective implementation of the AML/CFT/CPF compliance framework;
   iv. monitor the effectiveness and adequacy of the framework, including material deficiencies and remedial measures; and

v. ensure that the framework is periodically reviewed having regard to regulatory developments, emerging ML/TF/PF Risks and material changes in products, services, customer profiles, delivery channels, technology or business operations.

(b) Senior Management shall be responsible for the effective implementation of this Policy and shall ensure that appropriate systems, procedures, controls and resources are established and maintained. In the case of a Reporting Institution carrying on leasing business, this includes ensuring that the applicable AML/CFT/CPF and TFS controls are embedded in its leasing operations and all products, services and delivery channels through which such leasing operations are conducted.

(c) Senior Management shall ensure that material AML/CFT/CPF matters, control weaknesses, breaches and remediation plans are reported to the relevant Board on a timely basis. The Compliance Officer of each Reporting Institution shall also provide periodic reports to the relevant Board or Board committee on the implementation and effectiveness of the AML/CFT/CPF framework, at a frequency appropriate to the nature, size, complexity and ML/TF/PF Risk profile of the relevant Reporting Institution.

(d) Each member of the Group which is required by Applicable Law to appoint an AML/CFT/CPF Compliance Officer ("Compliance Officer") shall appoint an appropriately qualified person with sufficient seniority, authority, knowledge, resources and independence to discharge the functions of that office effectively.

(e) The Compliance Officer shall act as the central reference point for AML/CFT/CPF matters applicable to the relevant Reporting Institution and shall be responsible for overseeing the implementation and continued effectiveness of the relevant AML/CFT/CPF policies, procedures and controls.

(f) The Compliance Officer shall have independent authority to evaluate internally reported suspicious transactions and to determine whether a suspicious transaction report ("STR") is to be lodged with BNM's Financial Intelligence and Enforcement Department or such other authority as may be prescribed. No prior approval from the Board, Senior Management or any business function shall be required for the lodging of an STR.

(g) The Compliance Officer of each SKP-Regulated Entity shall coordinate with that entity's Person Responsible for Compliance appointed for purposes of the SKP regulatory framework.

(h) Where the same person holds more than one compliance role, the relevant member of the Group shall ensure that the arrangement does not impair that person's independence, capacity or ability to discharge the respective functions effectively and that any actual or potential conflicts of interest are appropriately identified, documented and managed.

(i) An independent review or audit of the AML/CFT/CPF framework shall be conducted at a frequency and scope commensurate with the relevant Reporting Institution's size, nature, complexity and ML/TF/PF Risk profile and in accordance with Applicable Law, subject to any exemption or simplification expressly available to that Reporting Institution. Material findings and corrective actions shall be reported to the relevant Board.

4. RISK-BASED APPROACH AND INSTITUTIONAL RISK ASSESSMENT

(a) Each Reporting Institution within the Group shall adopt a documented risk-based approach to identify, assess, understand, manage and mitigate the ML/TF/PF Risks to which it is exposed.

(b) The institutional risk assessment shall take into account all relevant risk factors, including:

i. customer and beneficial ownership profiles;
ii. products and services;
iii. transaction values, volumes and payment methods;
iv. countries and geographical exposure;
v. delivery channels, including face-to-face and non-face-to-face onboarding;
vi. agents, referral partners and other intermediaries;
vii. outsourcing arrangements;
viii. new or developing technologies; and
ix. in the case of a Reporting Institution carrying on leasing business, matters relevant to its leasing business including asset values, the nature and type of leased or rented assets, digital or other non-face-to-face onboarding and the nature and pattern of customer payments and transactions.

(c) Customers shall be assigned an appropriate ML/TF/PF risk rating in accordance with documented customer risk-rating criteria. The level and frequency of due diligence and monitoring shall be proportionate to the customer's assessed risk. Higher-risk relationships shall be subject to enhanced due diligence ("EDD") and such senior management approval as may be required by Applicable Law or the Group's procedures.

(d) The institutional risk assessment shall be reviewed periodically at a frequency commensurate with the relevant Reporting Institution's ML/TF/PF Risk profile and Applicable Law, and whenever there is a material change in the business, products or services, customer profile, geographical exposure, delivery channels, outsourcing arrangements or technology used by the relevant Reporting Institution.

(e) ML/TF/PF Risks arising from a new product, business practice, delivery mechanism or technology shall be assessed before its implementation or launch, and appropriate controls shall be established to manage and mitigate the identified risks.

5. CUSTOMER DUE DILIGENCE (CDD)

CDD shall be performed when establishing a business relationship, when suspicion exists regardless of amount, or when there is doubt about previously obtained information.

CDD shall also be renewed or refreshed where required by Applicable Law or the customer's risk profile, including where there is a material change in the customer's circumstances or the adequacy or reliability of previously obtained information is in doubt.

The relevant Reporting Institution shall identify and verify customers using reliable, independent documents/data and understand the purpose and intended nature of the relationship.

(a) Minimum CDD requirements

Customer	Minimum CDD information / control
Individual	Full name; NRIC/passport/official ID; residential/mailing address; date of birth; nationality; occupation; employer/self-employment/business; contact number; purpose and intended nature of the relationship; and such additional information as may be required by Applicable Law or the customer's risk profile. Identity must be appropriately verified.
Legal person / MSME	Name/legal form/proof of existence/unique identifier; registered/principal business address; nature of business; ownership/control; relevant senior management; authorised representative and authority; purpose and intended nature of the relationship; and such other information required to understand the customer's business and ownership/control structure.
Beneficial owner	Identify and take reasonable measures to verify natural persons who ultimately own/control the entity. The applicable cascading approach shall be followed by first identifying natural persons with controlling ownership interests (including, where applicable, ownership of more than 25%), followed by persons exercising control through other means and, where no such natural person is identified, the relevant natural person holding a senior management position.
Authorised representative	Verify the representative's identity and authority, including through an appropriate letter of authority, board resolution or equivalent evidence, before accepting instructions.
Sanctions / PEP / higher risk	Conduct applicable sanctions and politically exposed person ("PEP") screening and apply EDD where required, including obtaining source of funds and/or source of wealth information where relevant and required by Applicable Law or the assessed risk.

(b) Standard CDD shall be the minimum level of CDD applied by each Reporting Institution within the Group unless simplified CDD is expressly permitted under Applicable Law for the relevant circumstances.

(c) Where a customer relationship is established on a non-face-to-face basis, including through any website, application, electronic platform or other digital onboarding process, the relevant Reporting Institution shall implement appropriate measures to address the increased ML/TF/PF, fraud, operational and technology risks associated with such onboarding.

(d) The identity verification process shall be sufficiently robust to provide reasonable assurance as to the customer's true identity and shall incorporate appropriate independent verification, authentication, fraud detection and monitoring controls. Any non-face-to-face onboarding framework requiring Board approval under Applicable Law shall not be implemented until the requisite approval has been obtained.

(e) EDD shall be conducted where a customer, beneficial owner, business relationship or transaction presents higher ML/TF/PF Risk. EDD measures shall, where applicable, include obtaining additional identification information, additional information on the nature and purpose of the relationship, source of funds and/or source of wealth, senior management approval and more frequent or enhanced monitoring.

(f) Foreign PEPs, and their relevant family members and close associates, shall be treated in accordance with the EDD requirements prescribed under Applicable Law. Domestic PEPs and persons entrusted with prominent functions by international organisations shall be subject to appropriate risk assessment and EDD where the relationship is assessed as higher risk.

(g) Where the required CDD cannot be satisfactorily completed, the relevant Reporting Institution shall not establish or continue the business relationship or execute the relevant transaction, except to the extent otherwise permitted or required under Applicable Law. The Compliance Officer shall also consider whether the circumstances warrant the lodging of an STR.

6. ONGOING DUE DILIGENCE, SANCTIONS AND TRANSACTION MONITORING

(a) The relevant Reporting Institution shall conduct ongoing due diligence throughout the business relationship and shall keep customer and beneficial ownership information reasonably up to date. Transactions and activity shall be scrutinised to ensure that they are consistent with the Reporting Institution's knowledge of the customer, the customer's business and risk profile and, where relevant, the customer's source of funds.

(b) The relevant Reporting Institution shall maintain effective procedures to screen customers, potential customers, beneficial owners, authorised representatives and such other connected persons as may be required against applicable terrorism financing and proliferation financing sanctions and designation lists.

(c) Where a potential or confirmed match is identified, the relevant Reporting Institution shall promptly undertake the verification, freezing, blocking, rejection, reporting and other measures required under Applicable Law. No transaction shall be processed for a confirmed designated or sanctioned person except where expressly permitted by law or the relevant competent authority.

(d) The relevant Reporting Institution shall maintain appropriate manual and/or electronic systems and management information capable of identifying unusual, irregular or potentially suspicious activities or transactions having regard to the size, nature and complexity of its operations. Monitoring shall take into account, where relevant, the customer's risk profile, transaction patterns, cumulative activity, unusual values or volumes and internally established risk indicators or thresholds.

(e) Each Reporting Institution carrying on leasing business shall maintain documented AML/CFT/CPF red flags relevant to its leasing operations. Such red flags may include, without limitation, identity inconsistencies, unexplained third-party or unrelated payment instruments, unusual transaction volumes or quantities or values of leased or rented assets, rapid or repeated applications, transactions, cancellations or returns, suspected mule activity, unexplained ownership or control arrangements, abnormal refunds or chargebacks and attempts to circumvent customer identification or verification, screening or other compliance controls. The detailed red flags, thresholds and escalation criteria may be prescribed in the applicable AML/CFT/CPF procedures or implementation manual and updated from time to time to reflect emerging risks and typologies.

7. SUSPICIOUS TRANSACTION REPORTING AND CONFIDENTIALITY

(a) Employees shall report any activity or transaction which they know, suspect or have reasonable grounds to suspect may involve ML/TF/PF promptly through the designated secure internal reporting channel to the Compliance Officer (or, in the case of a member of the Group which has not appointed a Compliance Officer, such other person as may be designated for that purpose).

(b) Internal escalation is required regardless of the amount involved and shall include attempted transactions where circumstances give rise to suspicion.

(c) The Compliance Officer shall independently evaluate each internal report and determine whether there are reasonable grounds for suspicion. Where the applicable threshold for reporting is met, the Compliance Officer shall lodge an STR with the relevant authority promptly and within the timeframe prescribed under Applicable Law or by BNM from time to time.

(d) Where no reasonable ground is established, the decision and supporting evidence shall be documented and retained in accordance with this Policy and Applicable Law.

(e) STR information and related communications are strictly confidential. No director, officer, employee or representative shall disclose to a customer or any unauthorised person that an STR has been or may be lodged, that a suspicion has been formed, or any related information where such disclosure is prohibited under Applicable Law.

8. RECORD KEEPING, TRAINING AND REPORTING

(a) CDD, EDD, beneficial ownership, customer risk assessment, transaction, screening, correspondence, internal escalation, STR-related and other relevant AML/CFT/CPF records shall be maintained in a manner sufficient to permit the reconstruction of individual transactions and to demonstrate compliance with Applicable Law. As a minimum Group standard, such records shall be retained for not less than seven (7) years from the relevant date prescribed under Applicable Law, and for such longer period as may be required by any competent authority, investigation, prosecution, legal hold or other applicable requirement.

(b) Each Reporting Institution shall maintain appropriate screening procedures to ensure high standards of integrity when appointing directors, Senior Management, employees and persons performing relevant functions, to the extent required by Applicable Law and having regard to the nature and risk of the role.

(c) Appropriate AML/CFT/CPF and TFS training shall be provided to relevant directors, Senior Management, employees and representatives having regard to their respective roles and responsibilities. Training shall cover, where relevant, CDD, EDD, beneficial ownership, PEPs, sanctions, red flags, transaction monitoring, internal escalation, STR confidentiality and emerging ML/TF/PF risks. Attendance and training records shall be maintained.

(d) Where required under Applicable Law, the relevant Reporting Institution shall maintain an independent audit or review function to periodically assess the adequacy, effectiveness and compliance of its AML/CFT/CPF framework. Findings and remedial measures shall be reported to Senior Management and, where material, the relevant Board.

(e) The Compliance Officer, together with the relevant responsible functions, shall ensure that all AML/CFT/CPF regulatory reports, notifications and submissions applicable to the relevant Reporting Institution are prepared and submitted accurately and within the prescribed timeframes, including the applicable Data and Compliance Report ("DCR") or any replacement or successor reporting requirement.

(f) The relevant Reporting Institution shall maintain an appropriate regulatory and internal compliance reporting calendar identifying all recurring, periodic and event-driven AML/CFT/CPF reporting, assessment, review and notification requirements applicable to it.

9. OUTSOURCING AND THIRD PARTY SERVICE PROVIDERS

(a) The use of an agent, service provider, technology provider, screening provider or other third party shall not relieve the relevant member of the Group of responsibility for compliance with this Policy or Applicable Law.

(b) Where a material AML/CFT/CPF function is outsourced or supported by a third party, appropriate due diligence and contractual safeguards shall be implemented having regard to the nature and risk of the arrangement, including as applicable requirements relating to confidentiality, information security, access to records, audit rights, business continuity and regulatory access.

(c) Each member of the Group shall ensure that any outsourcing arrangement which is subject to an approval, notification or other regulatory requirement is dealt with in accordance with Applicable Law. Without limiting the foregoing, each SKP-Regulated Entity shall comply with the applicable SKP requirements in relation to outsourcing arrangements concerning its regulated leasing activities.

10. BREACHES, ESCALATION, MONITORING AND REVIEW

(a) The Policy Administrator shall ensure that appropriate records are maintained of the implementation of this Policy, including material exceptions, approvals, incidents, control deficiencies and corrective actions.

(b) Any material breach of this Policy or Applicable Law, repeated control failure, material ML/TF/PF exposure or matter which may cause material consumer, financial, regulatory or reputational harm shall be escalated promptly to the Compliance Officer and Senior Management and, where material, to the relevant Board or Board committee.

(c) The Compliance Officer and, where applicable, the Person Responsible for Compliance shall monitor regulatory developments relevant to this Policy and recommend such changes to the Policy, procedures, systems and controls as may be necessary.

(d) In respect of each SKP-Regulated Entity, any material change to this Policy or the related policies and procedures falling within Table 3 of the SKP Authorisation Standards shall be notified to SKP within the applicable regulatory timeframe.

(e) This Policy shall be reviewed at least annually and earlier where there is a material change in Applicable Law, the Group's business or risk profile, products or services,

customer profile, delivery channels, outsourcing arrangements, technology or identified ML/TF/PF risks.

(f) Any material amendment to this Policy shall be submitted to the relevant Board for approval before implementation, subject to any regulatory approval or notification requirements.

11. SUPPORTING AML/ CFT/ CPF PROCEDURES

(a) Each Reporting Institution within the Group shall maintain appropriate written procedures, standard operating procedures and/or an AML/CFT/CPF implementation manual to support the practical implementation of this Policy.

The supporting procedures of each Reporting Institution within the Group shall address, to the extent applicable, at least the following matters: institutional ML/TF/PF risk assessment; customer risk-rating methodology; CDD and eKYC; beneficial ownership; PEP and sanctions screening; EDD; ongoing due diligence and transaction monitoring; internal STR escalation and regulatory reporting; record keeping; personnel screening; training; independent review or audit; outsourcing; regulatory submissions including DCR; and such other matters required under Applicable Law. In the case of a Reporting Institution carrying on leasing business or an SKP-Regulated Entity, the supporting procedures shall additionally address such controls and operational matters as are relevant to its leasing activities and applicable SKP requirements.

(b) Operational matters including screening systems or vendors, internal reporting channels, system thresholds, risk-scoring parameters, internal forms and designated operational personnel may be maintained in the supporting procedures rather than this Policy and may be updated by Senior Management or the Compliance Officer within their respective authority, provided that any update which constitutes a material change to this Policy or which requires Board or regulatory approval or notification is dealt with accordingly.

-END-

Schedule 1 – Reporting Institutions and SKP-Regulated Entities

(as at the Effective Date, and as may be updated from time to time in accordance with paragraph 1(f))

1. ICT Zone Ventures Berhad (Registration No. 200101022505 (558263-V)) – Reporting Institution (leasing business) and SKP-Regulated Entity (applicant for authorisation from SKP under the Consumer Credit Act 2025).

Appendix A - AML operational decisions to complete before submission

Item	Decision / evidence
AML/CFT Compliance Officer	[Name, designation, appointment/BNM notification status]
Institutional ML/TF/PF risk assessment	[Attach / complete]
Customer risk-rating methodology	[Low/medium/high criteria]
Sanctions / PEP screening tool	[System/vendor/manual process]
CDD/eKYC evidence	[Map the applicable customer onboarding and eKYC information and controls against the relevant CDD requirements]
Internal STR channel	[Secure channel and internal review timeframe]
FINS / BNM reporting access	[Status]
Training plan	[Frequency / target staff]
Independent audit plan	[Frequency / auditor]
DCR submission owner	[ ]