

Basic Policy on Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing

RESPECT PAYMENT SERVICE Co., Ltd. (the “Company”), as a financial service provider conducting funds transfer business, recognizes that preventing money laundering, terrorist financing and proliferation financing is an essential responsibility for maintaining the soundness and integrity of the financial system.

The Company manages risks relating to money laundering, terrorist financing and proliferation financing and works to prevent them under the following basic policy.

1. Basic Approach

The Company considers AML/CFT/CPF measures one of its highest management priorities.

The Company seeks to prevent its products and services from being used to transfer criminal proceeds, fund terrorist activity, facilitate transfers related to the proliferation of weapons of mass destruction or serve other improper purposes.

While considering customer convenience, the Company prioritizes legal compliance and the integrity of the financial system and undertakes necessary checks, transaction restrictions and other measures.

2. Compliance with Laws and Regulations

The Company complies with the following laws, guidelines and rules:

- (1) Act on Prevention of Transfer of Criminal Proceeds and related laws and regulations
- (2) Payment Services Act and related regulations
- (3) Foreign Exchange and Foreign Trade Act and related regulations
- (4) Act on Special Measures Concerning Freezing of Property of International Terrorists and related regulations
- (5) Supervisory policies and guidelines issued by supervisory authorities
- (6) Notices, requests and alerts issued by relevant authorities
- (7) Other domestic and foreign laws and rules applicable to the Company

The Company continuously monitors legislative changes, international requirements, criminal methods and the external environment, and reviews its controls when needed.

3. Management Involvement

The board of directors and senior management are responsible for establishing and ensuring the effectiveness of the AML/CFT/CPF control framework.

Management performs the following functions:

- (1) Approving AML/CFT/CPF policies and material management standards
- (2) Reviewing risk assessments and mitigation measures
- (3) Assigning necessary authority to the responsible executive
- (4) Ensuring adequate personnel, budget, systems and expertise
- (5) Receiving reports on material cases and control issues

(6) Reviewing audits, testing and remediation progress

(7) Taking other measures required for effective controls

4. Management Framework

The Company designates an officer responsible for AML/CFT/CPF and clearly defines departmental roles and responsibilities.

The Company operates an effective three-lines-of-defense framework:

(1) First line of defense

Teams responsible for customer service, remittances, funds management and other operational functions perform day-to-day identification, customer management, transaction checks, detection and reporting of anomalies.

(2) Second line of defense

The compliance function performs risk assessments, establishes control standards, reviews transactions, monitors activity, advises and challenges operational functions, and tracks improvements.

(3) Third line of defense

The internal audit function independently audits the design and operation of the first- and second-line controls.

5. Risk-Based Approach

The Company identifies, assesses and mitigates its exposure to money laundering, terrorist financing and proliferation financing using a risk-based approach.

The risk assessment considers at least the following:

(1) Products and services

(2) Countries and regions served

(3) Customer characteristics, occupations, businesses and residence status

(4) Remittance purpose and source of funds

(5) Relationships with beneficiaries

(6) Transaction amounts, numbers, frequency and methods

(7) Disbursement and collection methods

(8) Overseas partners, financial institutions and contractors

(9) Non-face-to-face transactions, systems and new technology

(10) Past suspicious transactions, incidents, police inquiries and audit findings

(11) Domestic and international risk assessments, alerts and criminal trends

(12) Other factors necessary for identifying and assessing risks

The Company applies customer management, transaction checks, restrictions and other mitigations proportionate to assessed risks.

6. Customer Due Diligence

The Company verifies customer identity and transactions appropriately under applicable laws and internal standards.

For each customer, the Company verifies the following as appropriate:

- (1) Name, address, date of birth and other identifying particulars
- (2) Occupation or business activities
- (3) Purpose of the transaction
- (4) Source of funds
- (5) Destination country or region
- (6) Beneficiary and relationship to the customer
- (7) Beneficial owners, representatives and agents
- (8) Other facts needed to understand customer risk

The Company continually monitors customer information and transaction activity in accordance with risk and requests updates or additional evidence as needed.

7. High-Risk Customers and Transactions

The Company applies enhanced due diligence where risk is high owing to the customer, country or region, product, transaction method or other factors.

Enhanced due diligence may include:

- (1) Additional checks on identity and customer information
- (2) Detailed review of remittance purposes and circumstances
- (3) Verification of source of funds or financial position
- (4) Confirmation of relationships with beneficiaries
- (5) Senior-management approval
- (6) Restrictions on transaction frequency and amounts
- (7) Enhanced ongoing monitoring
- (8) Other measures necessary to reduce risks appropriately

Where necessary checks cannot be completed, the Company may suspend, restrict or refuse registration or transactions.

8. Economic Sanctions and Screening

The Company screens customers, beneficiaries, transaction parties, overseas partners and external contractors against official and other reliable information sources.

Where relevant, screening uses:

- (1) Official names of individuals and organizations
- (2) Names in Roman letters and other foreign scripts

(3) Commonly used names, aliases and former names

(4) Business or trading names

(5) Dates of birth or establishment

(6) Nationality, place of business and addresses

(7) Other information useful for identity resolution

If a sanctions match or potential match is detected, the Company stops the transaction, undertakes further checks and takes other legally required action.

9. Transaction Monitoring

The Company monitors transactions to detect suspicious or unusual activity in view of customer characteristics, transaction purposes, prior activity and other circumstances.

Additional scrutiny may be applied to:

(1) Transactions unusually large for the customer's characteristics or income

(2) Repeated transactions over a short period

(3) Transfers to numerous beneficiaries or multiple countries

(4) Transactions inconsistent with the declared purpose

(5) Third-party deposits or suspected transfers on behalf of others

(6) Transfers involving high-risk countries or regions

(7) Transactions materially inconsistent with normal customer activity

(8) Other suspicious or unusual transactions

10. Suspension, Restrictions and Refusals

The Company may temporarily hold transactions pending identification, customer information, remittance purpose, source of funds, beneficiary information, sanctions or other required checks.

The Company may refuse to start or continue a business relationship, impose restrictions or reject a remittance when:

(1) Legally required checks are incomplete

(2) The customer fails to provide required information or documentation

(3) Submitted information is false, forged or materially inconsistent

(4) The customer or transaction is subject to sanctions or restrictions

(5) Funds may be used for money laundering, terrorist financing or proliferation financing

(6) The Company's terms or management standards are breached

(7) Other circumstances make the transaction inappropriate

11. Suspicious Transaction Reports

The Company assesses potentially suspicious transactions in light of the nature of the transaction, customer characteristics, purpose, source of funds and relevant circumstances.

Where a transaction is determined to be suspicious, the Company files the required report with the competent authority under applicable law.

The Company does not disclose to customers or other parties that a suspicious transaction report has been filed or is being considered.

12. Management of Overseas Partners and Outsourcers

The Company undertakes appropriate due diligence and assessment of overseas partners and contractors before and during the contractual relationship.

The Company reviews the following as appropriate:

- (1) Licenses and legal compliance
- (2) AML/CFT/CPF controls
- (3) Economic sanctions compliance
- (4) Identity verification and transaction monitoring
- (5) Incidents, fraud and regulatory action
- (6) Information security and privacy
- (7) Subcontracting
- (8) Recordkeeping and cooperation with audits
- (9) Other aspects necessary to determine suitability

The Company retains ultimate management responsibility for AML/CFT/CPF even where work is outsourced.

13. Suitability of Officers and Employees

The Company ensures that officers and employees responsible for AML/CFT/CPF have appropriate knowledge, experience and suitability.

The Company prevents internal misconduct, misuse of information and ineffective controls through separation of duties, access controls, approval, review and other measures.

14. Training and Education

The Company trains officers and employees upon joining and periodically thereafter in:

- (1) The fundamentals of AML/CFT/CPF
- (2) Applicable laws and internal policies
- (3) Identity verification and customer due diligence
- (4) Economic sanctions and checks required under foreign exchange laws
- (5) Transaction monitoring and holds
- (6) Suspicious transaction reporting
- (7) Fraud and criminal methods
- (8) Record retention and confidentiality
- (9) Other matters relevant to their work

The Company records training and reviews employee understanding and practical application when necessary.

15. Records and Retention

The Company prepares and retains the following records under applicable laws and internal rules:

- (1) Identity verification and customer management records
- (2) Customer risk assessments
- (3) Transactions and remittances
- (4) Sanctions screening and review
- (5) Transaction monitoring and alert resolution
- (6) Transaction holds, releases and refusals
- (7) Suspicious transaction assessments and reports
- (8) Overseas partner and contractor management
- (9) Training, audit and remediation
- (10) Other records evidencing AML/CFT/CPF controls

16. Internal Audit

The internal audit function independently assesses AML/CFT/CPF controls, separate from operational and compliance functions.

Audits assess not only written procedures but also the effectiveness of customer management, transaction reviews, monitoring, suspicious transaction reporting, sanctions compliance, training and remediation.

Audit findings are addressed by designated responsible persons within established deadlines and the effectiveness of remediation is verified.

17. Assessment and Improvement of Controls

The Company periodically reassesses the effectiveness of its AML/CFT/CPF controls in light of legal changes, risk assessments, transactions, suspicious activity, incidents, audits, criminal methods and external changes.

Where improvements are needed, the Company promptly reviews policies, procedures, systems, training, staffing and other controls.

18. Cooperation with Authorities

The Company responds appropriately and lawfully to legitimate inquiries and requests from regulators, the police, investigators and other agencies.

The Company cooperates with financial institutions, funds transfer providers, overseas partners and other businesses to prevent crime and misuse, within the limits permitted by law and information-management rules.

19. Publication of this Policy

The Company publishes this Policy on its website or through other appropriate means.

20. Amendments

Adoption, material amendment or repeal requires approval of the board of directors.

Minor wording changes, legal updates and other changes that do not alter the substance may be approved by the representative director or compliance officer.

21. Former Policy

Former Policy 20-4, Basic Policy on Prevention of Money Laundering and Terrorist Financing, is repealed with effect from the commencement of this Policy.

The former policy is retained with revision records and comparison documents.

Adoption and Revision History

Established: January 11, 2017

Revised: March 31, 2026

Consolidated revision: July 21, 2026