English translation of the AML/CFT Guideline 2019 of Gaming Sector

Notes to users:

This English version is for reference only. The Chinese and Portuguese versions are the official version.

In the event of any discrepancies, the official version of the Instruction should always prevail.

DICJ Instruction No.1/2019

Preventive Measures for Anti-Money Laundering ("AML") and Combating Financing of Terrorism ("CFT")

In accordance with Article 4, paragraph 3, of the Administrative Regulation No.34/2003 and Article 2, paragraph 2 of Administrative Regulation No.7/2006, the Director of the Gaming Inspection and Coordination Bureau exercises the competency and issues this Instruction ("the Instruction"):

Article 1
Amendment of the Instruction No.1/2016

The articles 2,11,17 and 23 of the Instruction No. 1/2016 is amendment as follow:

«Article 2
Definitions

1) […].
2) […].
3) […].
4) […].
5) […].
6) […].
7) […].
8) […].
9) […].
10) […].
11) […].
12) […].
13) **Foreign politically exposed persons ('Foreign PEPs')**: Foreign *PEPs* are:

1) Individuals who are or have been entrusted with prominent public functions by a foreign country or outside Macau (SAR), China, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

2) Individuals who are or have been entrusted with a prominent function by an international organisation, namely the function of president, vice-president, director, deputy director, and members of the board or equivalent functions.

3) The definition also covers the close family members or close associates, and business associates of those individuals.

4) The politically exposed persons (PEPs) of Mainland China, Hong Kong Special Administrative Region of China, and other regions of China, are considered as foreign politically exposed persons for the purpose of this Instruction.

14) […].
15) […].
16) […].
17) […].
18) […].

Article 11
Reporting Suspicious Transactions

1. The addressees of this Instruction should, through the STRs, identify the participants and document the suspicious transactions, or attempted suspicious transactions, regardless of the amounts involved, as follows:
   1) […].
   2) […].
   3) […].
2. […].
3. Suspicious transactions should be reported to GIF, via the filling of STR, within two working days after the detection of the transaction.

Article 17
Inter property Transactions

1. […].
2. […].
3. […].
4. Without prejudice of other legal obligations, under the scope of group-level compliance as defined previously, in case of filing a suspicious transactions report (STR), this information can be shared over the entities of the same gaming group (e.g. parent companies, subsidiaries, representative offices, or agents), subject to previous authorization of the Gaming Regulator (DICJ), and under the following cumulative conditions:

   1) There is a risk analysis of money laundering and/or financial terrorism of the financial transaction or of the respective gaming activities performed;

   2) The risk analysis identified a conduct of a new type of typology to commit the money laundering crime or the finance terrorism crime;

   3) The conduct of the new type of typology is relevant on group-level compliance and information sharing within the same gaming group is appropriate to mitigate the inherent risk.

Article 23
Confidentiality

1. [..].
2. Employees of the Addressees of the Instruction, including its officers, board of directors or supervisors of casinos or any other gaming areas, are prohibited from tipping-off the submission of STRs to the GIF, and also the details of those transactions, to those who are involved in the suspicious transactions and any other persons or entities, with the exception of the legal regime addressed in paragraph 4 of Article 17.»

Article 2.
Republication

Its republish, on Annex, the Instruction n.1/2016, with all the current amendments approved with this Instruction.

Article 3.
Effective

This Instruction will be effective on January, 29, 2019.

Approved by the Director of DICJ on January 25, 2019.

Annex

(referred to in Article 2.)

REPUBLICATION

DICJ Instruction No.1/2016

Preventive Measures for Anti-Money Laundering ("AML") and Combating Financing of Terrorism ("CFT")

In accordance with Article 4, paragraph 3, of the Administrative Regulation No.34/2003 and Article 2, paragraph 2 of Administrative Regulation No.7/2006, the Director of the Gaming Inspection and Coordination Bureau exercises the competency and issues this Instruction ("the Instruction"):

Part I - General Provisions

Article 1
Objective of the Instruction

The Instruction defines the obligations, minimum internal control policies and procedures required for implementation by the gaming sector of the Macau SAR in order to prevent money laundering and financing of terrorism.

Article 2
Definitions

The followings are defined for the purpose of the Instruction:

1) **Beneficial owner** – refers to the natural persons (s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

2) **Money laundering** – the process of introduction and concealment of illicit money or assets into legitimate economic activities.

3) **Cheque** – a bill that bears an order of payment. The definition includes personal cheques, business company cheques, bank drafts, travellers cheques, cashier orders/cashier's cheques, and money orders.

4) **Compliance Officer** – an officer of the gaming concessionaires/sub-concessionaire or junket promoters of casino games of fortune who is mainly

responsible for ensuring implementation of AML/CFT preventive measures and compliance with the respective legal regimes.

5) **Gaming credit** – purchase of chips or other gaming instruments which are postponement of payment, as governed by the Law No.5/2004.

6) **Money laundering Crime** – purchase of value assets or properties by committing an act typified as a crime and specified in the Law No.2/2006 and punishable under such law.

7) **Financing of Terrorism Crime** – supplying or gathering of funds totally or partially for the practice of terrorist acts as typified and punishable as a crime under the Law No. 3/2006.

8) **Gaming Inspection and Coordination Bureau ("the DICJ")** – regulatory and supervisory authority bureau of the gaming sector, including casino games of fortune, pari-mutuel and gaming activities opened to the public under the concession administrative legal framework.

9) **Financial Intelligence Office (the GIF)** – the Office established under Executive Order No.227/2006 of August 7, with the function to collect, analyze and disseminate information with AML/CFT to the competent authorities in relation to money laundering and financing of terrorism.

10) **Gaming operations** – legal operations related to the land based casinos games of fortune, pari-mutuel or gaming activities opened to the public which are authorized by the Government of the Macau SAR, including placement of bets, winning payments, purchases and redemptions of chips, tickets or tokens, and granting or repayment of gaming credits.

11) **Suspicious transaction** – a gaming or wagering related activity which by its nature, unusual character or complexity, that indicates any activity of money laundering or financing of terrorism activity.

12) **Large-sum transaction** – operation relating to the practice of gaming or wagering with the value equal to or more than MOP500,000 (five hundred thousand patacas) or its equivalence in any other currency.

13) **Foreign politically exposed persons ('Foreign PEPs')**: Foreign *PEPs* are:

    1) Individuals who are or have been entrusted with prominent public functions by a foreign country or outside Macau (SAR), China, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.
    2) Individuals who are or have been entrusted with a prominent function by an international organisation, namely the function of president, vice-president, director, deputy director, and members of the board or equivalent functions.

3) The definition also covers the close family members or close associates, and business associates of those individuals.

4) The politically exposed persons (PEPs) of Mainland China, Hong Kong Special Administrative Region of China, and other regions of China, are considered as foreign politically exposed persons for the purpose of this Instruction.

14) **Domestic politically exposed persons ("Domestic PEPs")** – are individuals who are or have been entrusted with prominent public functions in the Macau SAR, such as the Chief Executive, members of the Government of the Macau SAR, members in the Executive Council, senior politicians, senior officials of governmental, judicial or military officials, and senior executives of corporations owned or controlled by the Macau Special Region. The definition also covers the close family members or close associates, and business associates of those individuals.

15) **Large-sum transactions report ("ROVE")** – a report to be executed by the addressees of the Instruction when the gaming activities reach the reporting threshold of large-sum transactions during the course of their operations. Please refer to the template attached in the Instruction.

16) **Suspicious transactions report ("STR")** – a report to be executed by the addressees of the Instruction when they detect a suspicious transaction during the course of their gaming operations. The template of the report is set out by the GIF.

17) **Stable business relationship** – any business or professional relationship established between the gaming concessionaires of casino games of fortune, pari-mutuel, or gaming activities open to the public, with the customers to which in the moment that is conducted is expected to be or to become permanent, and usually involves provision of services or offering products or services in a stable and continuous manner, and without regard the number of individual transactions to carry out or to be carried out.

18) **Occasional transaction** – any transaction carried out by any gaming concessionaire that is not within the definition of an established business relationship, namely a transaction that occurs on sporadic or isolated time basis, and without regard the actual number of transactions performed.

Article 3
Addressees of the Instruction

The addressees of the Instruction are:

1) The concessionaires and sub-concessionaires of the land based casino exploring games of fortune;

2) The management companies of the concessionaires or sub-concessionaires of the land based casino exploring games of fortune;

3) The junket promoters of games of fortune;

4) The concessionaires of pari-mutuel;

5) The concessionaires that offer gaming activities to the public (e.g. lotteries).

Article 4
AML/CFT Internal Control Policies and Procedures

1. The addressees of this Instruction should adopt internal controls policies and procedures to combat money laundering and terrorist financing, taking into account the applicable legal provisions of the Macau SAR, namely the Law No. 2/2006 and Law No. 3/2006, the Administrative Regulation No. 7/2006, Article 34 of Law No. 16/2001, Article 30 item 6 of the Administrative Regulation No. 6/2002, and others that may yet be approved in the future.

2. The internal control policies and procedures to be adopted by the addressees are subject to the prior approval by the DICJ.

3. Under the regulatory authority the DICJ have the power to require the addressees to revise their internal control policies and procedures on AML/CFT.

Article 5
Scopes of the AML/CFT Internal Control Policies and Procedures

The following (at a minimum) should be incorporated into the AML/CFT internal control policies and procedures, including but not limited to:

1) Identifying, assessing and understanding of the risks of money laundering and financing of terrorism inherent to their business as defined in Article 6;

2) The obligation to carry out customer due diligence ("CDD"), including identifying and verifying the identity of those who are involved in gaming activities and the respective financial transactions conducted within a stable business relationships, suspicious transactions or large-sum transactions;

3) Identifying the beneficiary owners in gaming activities and their respective financial transactions;

4) Identification and verification of PEPs, both foreign and domestic, identify their transactions and conduct a on-going monitoring over their transactions;

5) Controls over the issuance, acceptance and payment of cheques or other negotiable instruments with the patrons, and if applicable, the agents or persons who act on the patrons' behalf.

6) Controls over the movement of funds via domestic and cross-border wire transfers;

7) Identify and assess the risk of money laundering and terrorist financing that may arise in relation to the development of new products and services, or the use of new

technologies or those under development over new products or pre-existing products;

8) Detection of suspicious transactions and large-sum transactions;

9) Reporting suspicious transactions (STR's) to the GIF ;

10) Reporting of large-sum transactions (CTR's) to the DICJ;

11) Appointment of a compliance officer ("the Compliance Officer"), and respective substitute;

12) Providing training to employees who have the responsibility to carry out the AML/CFT internal control policies and procedures;

13) Ensuring confidentiality of AML/CFT information and reports;

14) Record Keeping of the documents for a minimum period of 5 years;

15) Duty to cooperate with competent authorities;

16) Defining the applicable penalties/sanctions in the event of non-compliance.

Article 6
Risk Assessment

1. The addressees of this Instruction should, every two years, identify, assess and understand the risks of money laundering and terrorist financing on their business activities and adopt adequate measures to mitigate those risks.

2. The addressees should adopt a risk-based approach to ensure that the measures taken are appropriate and proportionate to the risks identified, in order to enable AML/CFT resources to be allocated effectively.

3. In adopting the risk-based approach, the addressees should consider the following risk factors:
   1) National or geographical risk;
   2) Customer risk;
   3) Product/service risk;
   4) Risk associated with the nature of transactions or business relationship;
   5) Risk of delivery channels offered in the product/service;
   6) Risk of new technology.

4. In determining the AML/CFT measures to mitigate the risks, the addressees should also take into account the risks identified by the supervisory authorities and the GIF, or any other competent authority in the Macau SAR.

Article 7
Assessment of Effectiveness

The addressees of this Instruction should carry out regular assessment over their AML/CFT internal control systems to ensure the adequacy and effectiveness of the measures implemented.

Article 8
Supervision

Within the scope of the AML/CFT, the addressees of this Instruction are subject to the supervision of the DICJ, and also the compliance with their obligation to the GIF, based on the competencies of the two public authorities.

Part II - Preventive measures

Article 9
Identification and Verification of Identity

1. The addressees of this Instruction should undertake customer due diligence (CDD), including the obligation to identify and verify the identity of the following persons:
    1) Patrons or beneficiaries of gaming credits who are involved on a stable business relationship, suspicious transactions or large-sum transactions;
    2) Representatives or agents of the persons referred in the previous paragraph above;
    3) If there is knowledge that the patrons, gamblers or beneficiaries of gaming credits are acting on behalf of others, the persons on whose behalf they act for should also be identified;
    4) Beneficial owners of patrons who designate the patrons to act on their behalf through any forms of assignment;
    5) Any of the persons referred above whenever there are doubts about the validity and accuracy of the information being provided.

2. The identity of the natural person should be verified against original identification documents issued by official entities, namely identity cards, passports, travel documents, or any other equivalent credentials.

3. The (permanent) address can be proved by the identity documents referred above, or alternatively by documents issued by third parties, namely, work permits or

professional certificates, driving licenses, utilities bills, telephone bills or bank statements.

4. The identity of the above mentioned persons should be verified against the photographs in the official identity documents. With the prior consent of the respective Compliance Officer, other documents may be used in exceptional circumstances. In that case, the fact shall be documented and duly signed by the Compliance Officer for evidence.

5. The use of fictitious names, or maintaining business relationships previously established using anonymous identities, shall be strictly prohibited.

Article 10
Reporting Large-sum Transactions

1. The addressees of this Instruction should, through the ROVE attached in the Appendix, identify and verify the participants and report the following transactions:
   1) Gambling or wagering in the amount equal to or exceeding MOP500,000 (five hundred thousand patacas) or equivalent amount in any other currency;
   2) Provision or repayment of gaming credit in the amount equal to or exceeding MOP500,000 (five hundred thousand patacas) or equivalent amount in any other currency;
   3) Gambling, wagering, provision or repayment of gaming credit, individually less than the above reporting amount, but with an aggregated total within 24 hours that has reached or exceeded the threshold amount of MOP500,000 or equivalent amount in any other currency;
   4) Gaming promotion activities, including gaming settlement payment of the patron, or beneficiary owner, with an amount equal to or exceeding MOP 500,000.00 (five hundred thousand patacas) or equivalent amount in any other currency.

2. The report referred in the previous paragraph shall include at a minimum the following information:
   1) Name(s) of the person(s) involved;
   2) Gender;
   3) Date and place of birth;
   4) Nationality;
   5) Home address(es);
   6) Profession or occupation;
   7) Type of identity document;
   8) Date of the transaction;
   9) The transaction amount and source of funds;
   10) Beneficiary owner;

11) Methods of payments;

12) Signature of the Compliance Officer responsible for the execution or revision of the report.

3. The report shall be prepared within two working days following the completion of the transaction.

4. A copy of the ROVE must be sent to the DICJ in electronic format.

5. The electronic copies of the ROVEs shall be sent in aggregate to the DICJ on the 1st and 15th of each month.

Article 11
Reporting Suspicious Transactions

1. The addressees of this Instruction should, through the STRs, identify the participants and document the suspicious transactions, or attempted suspicious transactions, regardless of the amounts involved, as follows:

   1) Gambling or wagering that indicates an offense of money laundering crime or financing of terrorism crime, based on their nature, complexity, amounts involved, volume or unusual nature;

   2) Gaming credit that indicates an offense of money laundering crime or financing of terrorism crime, based on their nature, complexity, amounts involved, volume or unusual nature;

   3) Gaming promotion activities that indicate an offense of money laundering crime or financing of terrorism crime, based on their complexity, amounts involved, volume or unusual nature.

2. Where there are strong indications of money laundering crimes or financing of terrorism crimes, and the implementation of CDD measures in such situation may make those who perform the transactions know that they are in the course of administrative or criminal investigations related to money laundering or terrorist financing, non-implementation of CDD is allowed, however it is mandatory to report the incident through the filling of an STR.

3. Suspicious transactions should be reported to the GIF, via the filling of an STR, within two working days after the detection of the transaction.

Article 12
Completing and signing the ROVEs and STRs

1. ROVEs shall be completed and signed by the persons designated by addressees of this Instruction.

2. STRs shall be completed by the staff members of the addressees who detect the suspicious transactions during the course of their work.

3. Both types of reports mentioned in the preceding paragraphs should be reviewed thoroughly and signed by the Compliance Officer.

Article 13
Electronic reporting of ROVEs

1. The electronic reporting and submission of ROVEs shall be subject to approval by the DICJ.

2. The addressees of this Instruction should submit all the relevant required documents and information for the approval with a minimum of 60 days in advance, namely the electronic system to be used, internal control procedures, details of the network and database system, system security measures, details of the vendor and the risk assessment of the IT security.

3. The DICJ will define the specific terms and conditions for the abovementioned approval in compliance with this Instruction.

Article 14
AML/CFT Reporting by Junket Promoters

1. The ROVEs completed by the junket promoters should be reviewed and signed by the Compliance Officers of Concessionaires/Sub-Concessionaires of casino games of fortune who have the obligations to ensure the compliance of the AML/CFT measures.

2. The STRs reporting of junket promoters should be subject to special monitoring by the Concessionaires/Sub-Concessionaires of casino games of fortune.

3. Accordingly, the Concessionaires/Sub-Concessionaires should maintain the daily records of the numbers of STRs filed by the junket promoters, and monitor the compliance of the STR reporting obligation.

Part III - Enhanced Due diligence Duties

Article 15
Politically Exposed Persons ("PEPs")

1. The addressees of this Instruction should have an adequate risk management system to determine whether the customer or the patron, his/her representative or beneficial owner is a PEP.

2. Enhanced due diligence (EDD) must be performed for the identification and verification of identity of both domestic and foreign PEPs.

3. Enhanced on-going monitoring shall be carried out over the transactions of the PEPs, their representatives or their beneficial owner in order to determine the source of funds and to understand their financial and asset profile.

4. The acceptance or maintenance of the business relationships with PEPs should be subject to the approval by members of the board of directors, or persons engaged in management positions.

5. The obligations to PEPs should also be applied to family members or close associates of those PEPs.

Article 16
Enhanced Due Diligence related with the Risks of Operations

The addressees of this Instruction should carry out enhanced due diligence measures to their patrons, the representatives or the beneficial owner of those patrons that is adequate and proportionate to their risks identified, based on the nature of business relationship or type of transaction, and also the country risk, especially:

1) Countries that are identified as high risk by the FATF or any international organization which has similar role;
2) Countries that are subject to sanctions, embargoes or similar measures imposed by the United Nations, or countries that have been identified as highly corrupted or those with predominant criminal activities;
3) Countries with intense terrorist activity, or those referred to as financiers of terrorist organizations by any suitable international body (Examples of international organizations: the International Monetary Fund, World Bank, OECD, etc.).

Article 17
Inter property Transactions

1. The establishment and transfer of legal rights and interests over funds or any other means of payment of gaming transactions between the gaming concessionaires /sub-concessionaires and their related companies, in the same gaming group, in any jurisdiction, namely their parent companies, agents, subsidiaries or representative offices, where the funds or the means of payments are for the gaming activities in the Macau SAR, or settlement of other legal obligations, these operations should be subject to the prior approval by the supervisory authority (i.e. the DICJ). Enhanced due diligence stipulated in Article 21 shall be exercised in order to identify the source of funds and verify the identity of the holders and the beneficial owners.

2. The obligation to comply with the due diligence measures over the customer (i.e. the CDD) ultimately lies with the company incorporated in the Macau SAR that holds the (gaming) concession, and in compliance with the legal framework of the country where the transfer relates, the addressees should have the full powers at

any time and without delay to request the following from the counter-party of the abovementioned transfer:

1) All information necessary for the compliance of the Instruction;
2) Copies of documents being used for collecting the information required to complying with the legal duties.

3. To comply with this Article, the addressees shall also have control measures in place to verify the statutory CDD requirements applicable to the country of the transfer are equivalent to those enforced in the Macau SAR, and those CDD measures are being effectively and continuously applied. Where it is not the case, the risks of that country should be identified and measures should be applied to mitigate those risks.

4. Without prejudice of other legal obligations, under the scope of group-level compliance as defined previously, in case of filing a suspicious transactions report (STR), this information can be shared over the entities of the same gaming group (e.g. parent companies, subsidiaries, representative offices, or agents), subject to previous authorization of the Gaming Regulator (DICJ), and under the following cumulative conditions:

1) There is a risk analysis of money laundering and/or financial terrorism of the financial transaction or of the respective gaming activities performed;
2) The risk analysis identified a conduct of a new type of typology to commit the money laundering crime or the finance terrorism crime;
3) The conduct of the new type of typology is relevant on group-level compliance and information sharing within the same gaming group is appropriate to mitigate the inherent risk.

Article 18
Special Requirements on Negotiable Instruments

1. The use of negotiable instruments by patrons, their representatives and the beneficial owners are governed by Article 1064 and following in the Macau Commercial Code, and should be subject to special monitoring by the addressees of the Instruction.

2. Individual financial transactions related to a gaming contract or any other transactions associate within, where they are paid with negotiable instruments, must be recorded by the addressees of the Instruction individually, in order to identify the name of the issuer, its beneficiary, ultimate beneficiary of the instrument especially in the case of bearer issuer, the date of issuance, date of payment, the designated amount and if applicable, the side agreements involved.

3. Accordingly, the addressees of the Instruction should have a register to daily document the transactions associated with negotiable instrument and retain all respective information, based on the internal control procedures set out in Article 4 of the Instruction.

Article 19
Wire Transfers

1. Any domestic or cross-border wire transfers of funds through financial institutions or by authorized money service providers, regardless of the types of currency involved, must be accompanied by the following information:
   1) Name of remitter (payer);
   2) Bank account number of the remitter - if the payer's bank account is used for such remittance;
   3) Remitter's national identity card number, or his/her address, or his/her place and date of birth, or his/her patron identity number in the casino;
   4) Name of beneficiary (payee);
   5) Bank account number of the beneficiary - if the payee's bank account is used to receive the funds.

2. In case of absence of a bank account number, it should be registered the unique transaction reference that provides the audit trail of the transaction.

3. In batch file transfers, by which a single originator aggregated the funds for transfer to multiple individuals, all of the above information should be obtained in order to identify the name of the remitter and the beneficiaries and also to enable the full tracing of the funds.

4. The legal requirements under this Article are only mandatory when the financial transactions performed within a stable business relationship equal to or exceed MOP120,000 and when the occasional financial transactions equal to or exceed MOP 8,000.

Article 20
New Technologies

1. The introduction and use of authorized new technologies in the (gaming) concessions, in particular those used in new products or pre-existing products, and also the new delivery channels used in these products or services, shall be subject to enhanced due diligence, identification and preliminary assessment of the inherent risks of money laundering and terrorist financing crimes.

2. The addressees should exercise appropriate and effective measures to mitigate the potential risks identified in order to prevent money laundering and terrorist financing crimes.

Article 21
Scope of the Enhanced Due Diligence

The following are the control measures for the previous Articles related to enhance due diligence (EDD), without the exclusion of others measures:

1) Obtaining additional information about the patrons, their representatives or the beneficial owners, and also the respective transactions;
2) Implementing additional procedures in order to confirm the information obtained;
3) Obtaining senior management approval when entering into a stable business relationship, conducting occasional transactions or any other transactions;
4) Performing enhanced monitoring over those transactions in order to detect whether the source of funds and any other evidence available indicate an act of money laundering or terrorist financing, and accordingly reporting those incidents to the competent authority;
5) Increasing the frequency to update the (due diligence) information of the patrons, their representatives, and beneficial owners;
6) Exercising on-going monitoring and review over the business relationships, which shall be carried out by the personnel of the compliance function or any other personnel independent from involvement in any direct business relationship with the patrons, their representatives or the beneficial owners.

Part IV - Obligation to Refuse Transactions and Other Obligations

Article 22
Obligation to Refuse Transactions

1. The Addressees of this Instruction should refuse to carry out the transactions requested by the patrons, customers or their agents when they cannot obtain the information necessary to fulfil their identification and reporting obligations as required in Articles 9 to 21.
2. When the transactions referred to in the preceding paragraph are suspicious, STRs should be filed to the GIF, indicating the reasons for the refusal of those transactions.

Article 23
Confidentiality

1. The information from ROVEs and STRs should be classified as confidential and only personnel directly involved may have knowledge of the data recorded in those reports or in the respective supporting documentation.

2. Employees of the Addressees of the Instruction, including its officers, board of directors or supervisors of the casinos or any other gaming areas, are prohibited from tipping-off the submission of STRs to the GIF, and also the details of those transactions, to those who are involved in the suspicious transactions and any other persons or entities, with the exception of the legal regime addressed in paragraph 4 of Article 17.

Article 24

Document retention

1. The Addressees of this Instruction should keep all the following documents for a minimum of five years to enable access by competent authorities:
   1) Documents or copies of supporting documents identifying the patrons, beneficiaries of gaming credits, the agents or individuals on whose behalf the agents act for, whenever they are under a stable business relationship, reported in suspicious transactions or large-sum transactions;
   2) ROVEs, copies of the STRs and supporting documentation of those transactions, including all the written documents for the gaming credits;
   3) Supporting documentation for those suspicious transactions reported but not being filed to the GIF after the decision of the Compliance Officer.
   4) Other relevant documents that are essential to permit reconstruction of all the individual transactions in order to adequately provide evidence in criminal procedures.

2. The documents mentioned in previous paragraphs could be replaced by microfilm or transferred to digital format, once the applicable changes have been made (mutatis mutandis) for Articles 47, 48 and Paragraph 2 of Article 49 of the Macau Commercial Code.

3. The storage of abovementioned documents must be located in the Macau SAR and the information of the location should be sent to the DICJ, and the access of those documents should be available swiftly to any competent authority in the Macau SAR upon request.

4. If the addressees of the Instruction suspend or cease their operations, the document record keeping obligation should still prevail until the expiration of the 5-year retention period.

Article 25
Duty to Cooperate

The Addressees of this Instruction should provide all the information and documents requested by law enforcement authorities, judicial authorities and other competent authorities with competence in prevention of AML/CFT crimes.

Part V - Special CFT Preventive Measures

Article 26
Due diligence and Updating of Suspected Terrorists Database

1. The Addressees of this Instruction should take all the necessary measures to prevent entering into any kind of business or commercial relationship with person

suspected of terrorism, or those individuals designated as terrorists by domestic or international competent authorities.

2. A database with the list of designated terrorist suspects should be maintained and used for screening against the customer list (self-built database).

3. The Addressees of the Instruction can, as an alternative, choose to acquire a commercial database developed by specialized companies with recognition in the sector (3rd party commercial database).

4. In either situation above (Paragraphs 2 and 3), the Addressees are required to ensure that the database is constantly updated and contains, at minimum, the list of locally designated terrorists recognized by the competent local authorities, by the United Nations Security Council or any other international organization that exercises identical sanctions regimes.

5. Gaming Concessionaires and Sub-Concessionaires of casinos games of fortune should provide the database at no cost to junket promoters in their casino properties for cost effective reasons.

6. The Addressees of this Instruction should also:
   1) Execute identity screening with the abovementioned database before entering into a business relationship with a new customer ;
   2) Perform identity screening regularly and every time when there is an update to the list of designated persons mentioned above on the existing list of customers;
   3) Execute identity screening with the abovementioned database during payments, in particular those funds being transferred through financial institutions, in which cases the beneficiary payee in the bank instruction should be screened against the database.

Part VI - Compliance Function

Article 27
Function of AML/CFT Compliance

1. The Addressee of the Instruction should maintain an independent, permanent and effective compliance function, in order to ensure compliance with the legal and contractual obligations under the (gaming) legal regime of the respective concessions, and in particular ensuring compliance with AML and CFT requirements.

2. The Addressees should ensure adequate powers, means and resources are provided to the Compliance Function to perform the duties, and having the authority for timely access to all relevant information, in particular information related to

customer identification and due diligence, and the information required for reporting large-sum transactions and suspicious transactions.

Article 28
Compliance Officer

1. The Addressees of the Instruction must also appoint at least one Compliance Officer, and his/her substitute ("the Assistant Compliance Officer"), to be responsible for ensuring the compliance of the abovementioned obligations.

2. The Compliance Officer should be functionally independent to perform the AML/CFT duties, and should master at least one of the official languages of the Macau SAR, and have extensive knowledge of the local legal system.

3. The Compliance Officer and the name of the Assistant Compliance Officer should be submitted to the DICJ on a timely basis.

4. The DICJ can determine the replacement of the Compliance Officer based on the consideration of the person's suitability or technical capacity.

5. The DICJ may require an ad-hoc written examination, if necessary, to assess the technical competency of the person(s) to be appointed as Compliance Officer.

6. The Compliance Officer should coordinate the implementation of all AML/CFT policies and internal control procedures in order to prevent AML/CFT crimes, in particular:
   1) Participating in the designing of the internal control systems;
   2) Monitoring the internal control systems, constantly assessing the adequacy and effectiveness of those controls, and timeliness and efficiency of resources allocated;
   3) Ensuring involvement in the review of STRs and ROVEs to be submitted to the GIF and DICJ respectively;
   4) Ensuring the timeliness, adequacy, accessibility of information in relation to the internal control systems and their procedures;
   5) Participating in designing, monitoring and evaluation of AML/CFT internal training policies;
   6) Formulating and implementing the regular assessments mentioned in Article 7;
   7) Liaising with the judiciary authorities, law enforcement and supervisory authorities;
   8) Reporting to the board of directors and to the senior management of the company regarding the AML/CFT internal control deficiencies or weaknesses.

Article 29
Compliance Culture

1. The Addressee of the Instruction must build up a companywide culture for anti-money laundering and terrorist financing, and a practice to adhere to laws and business ethics throughout all hierarchical levels of the company. These duties should be specifically the obligation of the board of directors for legal persons, or the holders of gaming licenses in case of natural persons.

2. To implement AML/CFT culture over addressees who are under a company group, group wide control measures shall be established over different types of risks mentioned in Article 6 of the Instruction, and, where permitted by laws, set up information exchange mechanisms for the purpose of fulfilment of the CDD requirements.

Part VII - Training Duties

Article 30
Duty of Employee Training

1. The Addressees of the Instruction should organize training programs for all employees who have the responsibility to carry out the AML/CFT internal control policies and procedures, aiming at ensuring effectiveness of the preventive measures and internal controls procedures adopted and to achieve a proper understanding of the risks and typologies of money laundering and terrorist financing.

2. Refreshment on AML/CFT training should be organized at least every two years.

3. The Addressees of the Instruction shall submit to the DICJ, within 30 days before the start of the AML/CFT training program, the timetable and outline of different training courses, their manuals and *curriculum vitae* of trainers in order to assess whether the quality and timeliness of the contents of the trainings are in accordance with the internal training policy previously defined by the Compliance Officer.

Part VIII - Sanctions

Article 31
Standards of other Supervisory Authorities

The provisions in the Instruction do not prejudice or are hampered by the enforceability of other applicable regulations under the power of other supervisory authorities, namely those within the financial sector, and in particular the actions subject to sanctions, likely the cancelation, suspensions or revocation of any legal authorization to carry out financial operations.

Article 32
Administrative Sanctions

Without prejudice to one's criminal liability, the omission, fault or negligence of the obligation of customer due diligence, reporting, refusal of transactions, document retention, reporting of suspicious transactions or cooperation with law enforcement and supervisory authorities is considered as an administrative offense, and subject to the penalties and sanctions set out in Article 9 of the Administrative Regulation No. 7/2006.

Final Dispositions

Article 33
Repeal

The Instruction will revoke Instruction No.2/2006.

Article 34
Effective

The Instruction will be effective on May 13, 2016.

Approved by the Director of the DICJ on April 21, 2016.