

ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND SANCTIONS POLICY

HALCYON SUPER HOLDINGS BV

Status: FINAL

Version: 3.0

Date: 08 Apr 2025

Change/Approval History

Version	Date	Author	Approver	Notes
1.1	27 Jan 2025	LT		First Draft
1.2	13 Feb 2025	LT/CC		Update draft based on CC comments
2.0	28 Feb 2025	LT	PM	Version 2.0 Approved
2.1	08 Apr 2025	LT/AM		Update based on AM comments
3.0	08 Apr 2025	LT	PM/Board	Version 3.0 Approved

Signed: P. Manktelow
P. Manktelow (Apr 10, 2025 13:38 GMT+8)
Name: Peter Manktelow

TABLE OF CONTENTS

SECTION 1. INTRODUCTION & POLICY STATEMENTS	4
1.1 INTRODUCTION	4
1.2 APPLICABLE LAWS, REGULATION AND GUIDANCE	5
1.3 BREACHES AND EXCEPTION HANDLING	5
1.4 ADMINISTRATION	6
SECTION 2. MONEY LAUNDERING, TERRORIST FINANCING & PROLIFERATION FINANCING	7
2.1 WHAT IS MONEY LAUNDERING?	7
2.2 WHAT IS TERRORIST FINANCING?	7
2.3 WHAT IS PROLIFERATION FINANCING?	8
2.4 WHAT ARE FINANCIAL SANCTIONS?	8
SECTION 3. RISK-BASED APPROACH AND RISK ASSESSMENT	9
3.1 RISK-BASED APPROACH	9
3.2 AML/CFT INSTITUTIONAL RISK ASSESSMENT	9
3.3 NEW PRODUCT AND SERVICE RISK ASSESSMENT	10
3.4 CUSTOMER RISK ASSESSMENT	10
SECTION 4: ROLES AND RESPONSIBILITIES	11
4.1 THE BOARD OF DIRECTORS	11
4.2 THE SENIOR MANAGEMENT	11
4.3 THE COMPLIANCE OFFICER	12
4.4 ALL EMPLOYEES	13
SECTION 5. KNOW YOUR CUSTOMER (“KYC”) AND CDD OBLIGATIONS	14
5.1 KYC AND CDD MEASURES	14
5.2 CUSTOMER NAME SCREENING	17
5.3 CUSTOMER RISK ASSESSMENT	18
5.4 ENHANCED DUE DILIGENCE	18
5.5 SIMPLIFIED DUE DILIGENCE	19
5.6 BUSINESS RELATIONSHIPS WITH PEPS	20
5.7 PROHIBITED RELATIONSHIPS	20
5.8 INTERNET PROTOCOL (“IP”) GEOFENCING	21
SECTION 6. ONGOING MONITORING OF CUSTOMER RELATIONSHIPS	22
6.1 ONGOING MONITORING INTRODUCTION	22
6.2 PERIODIC REVIEWS	22
6.3 TRIGGER EVENT REVIEWS	22
6.4 ONGOING SCREENING	22
6.5 IP GEOFENCING	23
6.6 OTHER CONTROLS	23
SECTION 7. BLOCKCHAIN ANALYTICS AND TRANSACTION MONITORING	24
7.1 TRANSACTION MONITORING	24
7.2 BLOCKCHAIN ANALYTICS SCREENING	24
7.3 MANUAL ESCALATIONS	24
SECTION 8. INVESTIGATION OF UNUSUAL ACTIVITY AND UTR FILING	25

8.1	INTERNAL ESCALATIONS OF POTENTIALLY UNUSUAL TRANSACTIONS	25
8.2	DETERMINATION OF UNUSUAL TRANSACTIONS	25
8.3	FILING A UTR	26
8.4	PROHIBITION OF DISCLOSURE / TIPPING OFF	26
8.5	POST-UTR FILING PROCEDURES	26
	SECTION 9. MANAGEMENT INFORMATION AND EXTERNAL REPORTING	28
	SECTION 10. EMPLOYEE SCREENING	29
	SECTION 11. RECORD KEEPING	30
	SECTION 12. TRAINING	31
	SECTION 13. QUALITY ASSURANCE (“QA”), COMPLIANCE TESTING AND INDEPENDENT AUDIT	32
13.1	QA AND COMPLIANCE TESTING	32
13.2	INDEPENDENT AUDIT	32
13.3	EXAMINATIONS BY THE GCB	33
	APPENDIX 1. DEFINITIONS	34

SECTION 1. INTRODUCTION & POLICY STATEMENTS

1.1 INTRODUCTION

- (a) Halcyon Super Holdings BV, is a company incorporated with limited liability in Curacao, (“Halcyon” or the “Company”). It owns and operates cloudbet.com - a gaming website offering an online sportsbook and casino where customers can place bets primarily in cryptocurrencies. Halcyon has an application for a gaming license in progress with the Curacao Gaming Control Board (“GCB”). Until that process is concluded, based on a transitional arrangement, the company is permitted to continue its operations under a Certificate of Operation issued by the GCB.
- (b) Halcyon is committed to operating its business in compliance with all applicable laws, regulations and regulatory guidance. One of these legislative requirements is to have systems and controls in place to prevent, detect and disclose financial crime risks, such as money laundering (“ML”), terrorist/proliferation financing (“TF”/“PF”), sanctions, corruption and other financial crime related illegal activity (collectively “ML/TF”).
- (c) The purpose of this Anti-Money Laundering (“AML”), Counter-Terrorist Financing (“CFT”) and Sanctions Policy (this “AML/CFT Policy” or “Policy”) is to comply with these legislative requirements, while providing clear minimum standards and guidance for Halcyon and its staff to enable them to meet their personal and corporate obligations for the prevention of ML, TF/PF, sanctions, corruption, and other financial crime related illegal activity (collectively “AML/CFT”).
- (d) The implementation of the standards and controls as set out in the Policy is critical in ensuring that ML/TF risks are managed effectively in compliance with legislative requirements. Failure to comply with AML/CFT legislation could result in financial penalties being levied against the Company, as well as the loss of the Company’s licence to conduct business and/or convictions against employees.
- (e) The Policy applies to all activities of Halcyon and forms part of Halcyon’s governance framework. It is applicable to all staff of the Company, inclusive of all officers, directors, managers, administrators and support staff and is not limited to individuals working under a contract of employment but also includes temporary/contract staff and consultants.
- (f) Non-compliance with this Policy is a serious matter that may lead to disciplinary action, up to and including dismissal.

1.2 APPLICABLE LAWS, REGULATION AND GUIDANCE

- (a) The Policy has been written to take into account, at a minimum, the following laws, regulations and guidelines:
 - (i) National Ordinance on identification when rendering services (“NOIS”)
 - (1) Primary AML legislation established by the Government of Curacao.
 - (ii) National Ordinance reporting unusual transactions (“NORUT”)
 - (1) Primary AML legislation established by the Government of Curacao.
 - (iii) Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction issued by the Curacao GCB (“AML/CFT Regulations”)
 - (1) The GCB has been appointed as the supervisory authority for AML/CFT compliance for the whole Curacao gaming sector. They have issued this guidance on AML/CFT, which takes into account the laws and expectations of the Government of Curacao and the recommendations of the Financial Action Task Force (“FATF”).
- (b) Furthermore, the Policy is additionally based on the key elements of the following Sanction Regimes (irrespective of whether global application is required by Curacao law):
 - (i) Sanctions imposed by Curacao under the Sanctions National Ordinance and Kingdom Sanction Act;
 - (ii) Sanctions imposed by the United Nations (“UN”);
 - (iii) Sanctions imposed by the European Union (“EU”); and
 - (iv) Sanctions imposed by the Office of Foreign Assets Control (“OFAC”) in the United States of America (“US”).

1.3 BREACHES AND EXCEPTION HANDLING

- (a) Any breaches of this Policy must be reported as soon as possible to the Compliance Officer (“CO”). The CO will be responsible for notifying senior management, as well as any regulatory reporting or mitigation plans resulting from the breach.
- (b) Applications for exceptional handling regarding this Policy may be made to the CO. Applications must be made in writing and outline the proposed approach, including any risk mitigation. As a general rule such applications will only be approved in rare circumstances, where there is no resulting breach of local regulatory requirements and risk mitigation is in place.

1.4 ADMINISTRATION

- (a) This Policy is owned by the CO and will be reviewed at least annually or more frequently when there are significant regulatory or business changes that will impact the Company.
- (b) This Policy must be reviewed and approved by senior management and the Board prior to implementation. All subsequent amendments to this Policy will similarly require senior management and the Board's review and approval.
- (c) This Policy is effective as of the date set forth in this document.
- (d) This Policy has been communicated to all relevant employees and all questions regarding this Policy should be directed at the CO, who can be contacted at compliance@cloudbet.com.

SECTION 2. MONEY LAUNDERING, TERRORIST FINANCING & PROLIFERATION FINANCING

2.1 WHAT IS MONEY LAUNDERING?

- (a) Money laundering is the process by which criminals seek to disguise the origin and true source of their illegal income to make it appear to have originated from a legitimate source (i.e. making dirty money look clean). Criminals launder money so they can avoid detection by law enforcement authorities and make personal use of illicit proceeds.
- (b) Money laundering consists of three stages:
 - (i) *Placement* – During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requests for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
 - (ii) *Layering* – This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
 - (iii) *Integration* – The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.
- (b) Most people think that money laundering refers to funds acquired from drug trafficking, but there are many predicate offences for money laundering such as human trafficking, arms trafficking, robbery, fraud, corruption, kidnapping and tax crimes.

2.2 WHAT IS TERRORIST FINANCING?

- (a) Terrorist financing can be defined as providing funds to an organization with the intention that they should be used, or the knowledge that they are to be used, to commit a terrorist act (i.e. an act to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act).
- (b) The main difference between financing of terrorism and money laundering involves the origin of funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. While money laundering is concerned with

obscuring the source of funds, terrorist financing is mostly concerned with obscuring the end recipient of the funds.

2.3 WHAT IS PROLIFERATION FINANCING?

- (a) Proliferation financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

2.4 WHAT ARE FINANCIAL SANCTIONS?

- (a) Financial sanctions are restrictions put in place by Intergovernmental Organisations (i.e. the UN) or Countries to achieve a specific foreign policy aim (e.g. to prevent conflict or respond to emerging or current crises). They often involve requirements to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities.

SECTION 3. RISK-BASED APPROACH AND RISK ASSESSMENT

3.1 RISK-BASED APPROACH

- (a) The risk-based approach (“RBA”) is central to the effective implementation of an AML/CFT program. It aims to ensure that efforts and resourcing are allocated appropriately to the highest areas of risk.. By adopting a risk-based approach, the Company is able to ensure that measures to prevent or mitigate ML/TF are commensurate with the nature and level of identified risks to which it is exposed to. This will allow the Company to focus its AML/CFT efforts in the most effective way.

3.2 AML/CFT INSTITUTIONAL RISK ASSESSMENT

- (a) The Company adopts a RBA to its AML/CFT framework and it is designed to be commensurate to the levels of risk posed by its business model.
- (b) The institutional risk assessment process is an integral part of the Company’s AML/CFT risk management framework and is completed on an at least annual basis (or more frequently where there are major changes to the external operating environment or internal business activities). It is used to tailor the AML/CFT framework to ensure that the Company has the appropriate resources, policies, procedures and controls in place to mitigate, as far as reasonably practicable, the risks identified.
- (c) The risk assessment follows applicable standards and methodologies, including amongst other things the clear identification of inherent risks derived from the following risk categories:
 - (i) Customer and Other Business Partner Risk;
 - (ii) Geographical Risk;
 - (iii) Product/Service and Transaction Risk;
 - (iv) Delivery/Distribution Channel Risk; and
 - (v) Other Relevant Qualitative Risk Factors.
- (d) In addition to the risk factors above, the risk assessment covers any findings/observations from control testing, internal audit, etc. It also considers outcomes and recommendations of the Curacao National Risk Assessment.
- (e) The inherent risk is compared with the assessment of the current AML/CFT framework and respective control environment, which includes all relevant measures, safeguards and controls implemented to counteract the inherent risks. Based on the ability of the AML/CFT framework to mitigate the inherent risks, a residual risk is calculated and, if necessary, an action plan is created to follow-up on any unmitigated risks that fall outside of the Company’s risk tolerance.

- (f) The risk assessment, including all subsequent updates, are documented and approved by the Company's Board of Directors.

3.3 NEW PRODUCT AND SERVICE RISK ASSESSMENT

- (a) The Company adopts a RBA to mitigate risks from the introduction of new products and services, including new business practices, new delivery mechanisms and the introduction of new or developing technology. This allows the Company to design appropriate controls that are commensurate to the levels of risks posed to the Company.
- (b) The Company assesses the ML/TF risk inherent in the development and introduction of any new products, services or business practices, as well as when looking to use new or enhanced technology solutions. This involves evaluating any new products and services in advance and adequately recording the risks and controls to mitigate them.

3.4 CUSTOMER RISK ASSESSMENT

- (a) The Company adopts a RBA to assess the risk profile of its customers, which is detailed in the customer risk assessment section below (Section 5.3). Based on the information and documentation provided at onboarding and collected from other sources, a customer is assigned with a risk rating that is commensurate with its risk profile. Higher risk ratings will require additional due diligence measures and a higher periodic review frequency.
- (b) The risk assessment methodology, and any subsequent updates to it, are approved by the Company's Board of Directors.

SECTION 4: ROLES AND RESPONSIBILITIES

4.1 THE BOARD OF DIRECTORS

- (a) The ultimate responsibility for ensuring the Company's policies, procedures and controls for preventing and detecting ML/TF are appropriately designed and implemented remains with the Company and the Board of Directors ("Board").
- (b) The Board has primary responsibility for the following:
 - (i) Ensuring the Company has an effective AML/CFT program and oversight framework that is reasonably designed to ensure compliance with applicable laws and regulations;
 - (ii) Establishing and approving the AML/CFT program, including establishing clear policies regarding management of key AML/CFT risks and approving the AML/CFT Policy, Institutional Risk Assessment and Customer Risk Assessment Methodology;
 - (iii) Overseeing the structure and management of the compliance operations; and
 - (iv) Setting the culture of compliance for the Company.

4.2 THE SENIOR MANAGEMENT

- (a) The senior management is responsible for the implementation of this Policy. In particular, senior management has responsibility for the following:
 - (i) Ensuring the Company's compliance with relevant AML/CFT laws and regulations, including ensuring that this Policy is reviewed on an annual basis and any changes are reported to the Board for approval;
 - (ii) Identifying, assessing and effectively mitigating ML/TF risks associated with the Company's customers, products, services and transactions;
 - (iii) Promoting and enforcing high standards of integrity;
 - (iv) Ensuring that all employees are adequately trained, so that they understand relevant compliance standards and adhere to them;
 - (v) Ensuring that relevant appropriate AML/CFT controls and monitoring procedures are in place;
 - (vi) Establishing mechanisms for appropriate escalation of AML/CFT issues;
 - (vii) Ensuring independent testing is carried out to assess the effectiveness of the AML/CFT program;
 - (viii) Reacting promptly and effectively to any compliance issues that arise;
 - (ix) Ensuring adequate resources across the Company are devoted to monitor the AML/CFT program and implement appropriate procedures and controls, in particular, that the appointed CO is not obstructed in the execution of their duties;

- (x) Ensuring that an Institutional Risk Assessment has been carried out and documented annually, with the results reported to the Board for approval;
- (xi) Ensuring that the Customer Risk Assessment Methodology, including any subsequent updates, are reported to the Board for approval; and
- (xii) Providing the Board with periodic reporting on the AML/CFT program, to keep them up to date and abreast of the current risks and strength of the implemented controls.

4.3 THE COMPLIANCE OFFICER

- (a) The Company has appointed a CO, who will be responsible for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the Board and senior management to ensure that ML/TF risks are adequately managed, in particular, the CO (or his delegate) has responsibility for the following:
 - (i) Overseeing the design and implementation of an effective AML/CFT program based on an analysis of the ML/TF risks faced by the Company;
 - (ii) Developing and monitoring the AML/CFT program to ensure it remains up-to-date and meets current applicable laws and regulations;
 - (iii) Overseeing all aspects of the Company's AML/CFT program, including monitoring effectiveness and enhancing the controls and standards where necessary;
 - (iv) Reporting on the operational effectiveness of the AML/CFT program, including trends and themes regarding unusual transaction reporting, to senior management and the Board and to make suggestions for improvements where appropriate;
 - (v) Supporting and advising all business units in the implementation of this Policy;
 - (vi) Drafting and maintaining the Company's policies and procedures for AML/CFT;
 - (vii) Designing and conducting the Institutional Risk Assessment on annual basis;
 - (viii) Designing and implementing the new product/service risk assessment framework and processes;
 - (ix) Overseeing the standards applied for customer onboarding (e.g. customer due diligence ("CDD"), name screening, customer risk assessment, enhanced due diligence ("EDD") and approvals);
 - (x) Ensuring transaction monitoring and screening processes are in place and effective (e.g. blockchain screening, customer transaction monitoring, manual escalations of unusual activity and travel rule application);
 - (xi) Monitoring and responding to legal and regulatory developments in relation to AML/CFT;

- (xii) Responding to queries and information requests from applicable regulatory authorities/law enforcement agencies;
 - (xiii) Planning, conducting and monitoring the internal training on combatting money laundering and terrorist financing; and
 - (xiv) Overseeing the Company's record keeping processes as they relate to AML/CFT.
- (b) The CO will also be responsible for the identification, evaluation and reporting of unusual transaction activity, in particular, the CO has responsibility for the following:
- (i) Reviewing internal escalations and determining whether or not it is necessary to make an unusual transaction report ("UTR") to the Curacao FIU, including any post filing obligations (i.e. blocking/freezing user accounts);
 - (ii) Maintaining all records relating to such internal reviews;
 - (iii) Providing guidance on how to avoid "tipping off" if any disclosure is made; and
 - (iv) Acting as the main point of contact with relevant authorities and law enforcement in relation to UTRs.

4.4 ALL EMPLOYEES

- (a) All employees are responsible as part of their duties, to do the following:
- (i) Acknowledging that failure to comply with this Policy can result in regulatory or legal measures against the Company and its employees and, in addition, internal sanctions may be imposed for any breaches;
 - (ii) Familiarizing themselves with this Policy and other policy and procedures under the AML/CFT program and comply with them at all times;
 - (iii) Understanding the AML/CFT policies that are applicable to their business unit and apply them to their policies and procedures;
 - (iv) Participating in any AML/CFT training provided by the Company;
 - (v) Reporting any actual, suspected or potentially unusual activity immediately to the CO in accordance with this Policy or any other operational procedures issued under the AML/CFT program; and
 - (vi) Reporting any actual or suspected breaches of, or attempts to bypass, the AML/CFT Policy to the CO.

SECTION 5. KNOW YOUR CUSTOMER (“KYC”) AND CDD OBLIGATIONS

5.1 KYC AND CDD MEASURES

(a) KYC and CDD involves collecting all information required to allow adequate assessment of the background of the customer and their expected transactions. It comprises the following principles:

(i) Identifying the customer (i.e. the person the Company is establishing a business relationship with or is carrying out an occasional transaction for) and, where applicable, the customer’s controlling person(s) and beneficial owners¹:

(1) For individual person customers, at a minimum, the following information will be collected²:

- a) Full name;
- b) Permanent residential address;
- c) Date of birth;
- d) Place of birth;
- e) Nationality; and
- f) Identity number.

(2) For Operational Legal Entity Customers³, at a minimum, the following information will be collected:

- a) Full legal name;
- b) Legal form;
- c) Permanent operating address, and postal address, if applicable;
- d) Date of incorporation;
- e) Place of incorporation;
- f) Type of business activity and detailed description of business;
- g) Full name of the relevant related parties of the legal person or arrangement (e.g. intermediate owners, directors in a company, partners in a partnership, settlor(s)/trustee(s)/beneficiary(ies) of a trust);

¹ Individual customers need to be the beneficial owner of the assets held within their Cloudbet account. The Company does not allow accounts to be opened for individuals with a Power of Attorney, or other such arrangements, where control is given to a person who is not the beneficial owner of the assets held with the Cloudbet account.

² In low risk scenarios the Company may limit identification to the three personal details set out in (a) to (c) in the below list.

³ Requirements for other forms of legal entities (i.e. unincorporated entities, trusts, foundations, associations, etc.) are detailed in the Customer Onboarding Procedures.

- h) Full name, permanent residential address, date of birth, place of birth, nationality and identity number of the individual authorised to act on behalf of the legal entity ("Authorised Person") (if applicable); and
- i) Full name, permanent residential address, date of birth, place of birth, nationality and identity number of the ultimate beneficial owner ("UBO"), meaning the individual owning, directly or indirectly, at least 25% of the capital or voting rights in the legal entity or otherwise controls it.
 - i) If there is no UBO identified as described above, an individual who exercises control of the legal entity by other discernable means will be identified. If no controlling individual according to this definition can be determined, the highest senior managing official will be identified.
 - ii) An exception to this requirement is given in situations where the legal entity is a listed company, public authority or regulated financial institution (i.e. simplified due diligence ("SDD")).
- (ii) Verifying the customer's identity, and where applicable, taking reasonable measures to verify the customer's controlling person(s) on the basis of reliable and independent information, data or documentation:
 - (1) For individual person customers the following verification methods may be used:
 - a) Perform biometric verification on the customer by comparing their verified unexpired government-issued identification document containing photographic evidence of the customer's identity (e.g. passport, identity card) with a liveness video check.
 - b) Where the identity document does not allow verification of the customer's residential address, collect proof of address documentation⁴ or verify through checking telephone directories, companies registries or reputable news sources.
 - (2) For operational legal entity customers the following verification methods may be used:

⁴ Recent (i.e. not older than 6 months) bank statement, utility bill (for phone bills, only fixed line telephone bills are accepted), letter from a public authority or rental agreement.

- a) The original or certified copy of the Certificate of Incorporation;
 - b) Memorandum and articles of association;
 - c) Authorisation Letter to open an account and confer authority to those who will operate it;
 - d) A search of the customer's file at a company registrar (i.e. by means of a current register extract issued by the registrar, by means of a written extract from a database maintained by the registrar, a supervisory body, or a trustworthy private individual);
 - i) Legal entities and partnerships that are not entered at a company registrar must be verified by means of a written extract from a database maintained by a registrar, a supervisory body, or a trustworthy private individual or copies of the articles of association (or equivalent document).
 - ii) Where the legal entity is a public company or is directly or indirectly associated with a public company, this fact may be documented instead of carrying out the verification procedure described above (i.e. SDD).
 - e) Verify the identity of the UBO(s) and Authorised Person(s) by referencing an unexpired government-issued identification document containing photographic evidence of the customer's identity (e.g. passport, identity card); and
 - f) Where the identity document does not allow verification of the individuals residential address, verify the address of the UBO(s) and Authorised Person(s) by collecting a proof of address document⁵ or verify through checking telephone directories, companies registries or reputable news sources.
- (iii) Understanding the purpose and intended nature of the business relationship. In the context of the gaming industry the purpose behind the business relationship is self-evident, so this principle includes obtaining further information, and, where possible, and reasonable, documentation to ascertain the customer's expected deposit and betting activity, source of funds ("SOF") for the assets to be deposited onto the platform and source of wealth ("SOW").

⁵ Recent (i.e. not older than 6 months) bank statement, utility bill (for phone bills, only fixed line telephone bills are accepted), letter from a public authority or rental agreement.

- (1) The Company may also use data collected over a period of time, from a range of customers, to create the profile of an average customer. Where the transactional patterns deviate from the average, other SOW information and documentation may be requested.
- (b) The KYC and CDD measures apply to all customers that withdraw USD2,200 (the equivalent of Naf. 4,000) within a 24 hour timeframe. They may also be applied in situations where a higher ML/TF risk is noted with the business relationship, even where the withdrawal threshold is not met. The extent of these measures may be subject to change to the extent permitted or required by regulatory requirements in line with the ML/TF risks associated with the business relationship.
- (c) The KYC and CDD measures will be applied at the time the threshold is reached and the user will not be able to withdraw their funds until the KYC and CDD measures are completed.
- (d) The business relationship will be terminated where the Company is unable to complete the KYC/CDD and, if applicable, EDD measures.
 - (i) Where there are grounds giving rise to suspicion of ML/TF, the case will be escalated to the CO for review. The CO will review the case in accordance with the Company's investigation procedures which are detailed in Section 8 below.
 - (ii) Where there is no reason for the retention of funds, the funds are to be sent back to the terminated customer as part of the offboarding process.

5.2 CUSTOMER NAME SCREENING

- (a) Customer name screening is performed as part of the KYC and CDD process, and, where applicable, the controlling person(s) and other relevant parties of a legal entity or arrangement.
- (b) Customer name screening is conducted against the following lists:
 - (i) Relevant Sanctions Lists:
 - (1) Sanctions imposed by Curacao under the Sanctions National Ordinance and Kingdom Sanction Act;
 - (2) Sanctions imposed by the UN;
 - (3) Sanctions imposed by the EU; and
 - (4) Sanctions imposed by OFAC in the US.
 - (ii) PEP Lists; and
 - (iii) Relevant Law Enforcement Lists.
- (c) All lists are maintained by a third party service provider and are updated in accordance with the service level agreement ("SLA") that has been executed with them.

- (d) Level 1 review of the alerts is conducted by the Customer Support Team, with Level 2 reviews handled by the CO.

5.3 CUSTOMER RISK ASSESSMENT

- (a) Each customer is assigned an AML/CFT customer risk assessment score according to the parameters defined in the customer risk assessment methodology. This customer risk assessment score is a numerical representation of the relative risk of each customer based on information gathered during KYC/CDD.
- (b) The customer risk assessment methodology assigns relative weights to risk score parameters that are then totalled to arrive at a customer risk assessment score of Low, Medium, or High. This customer risk assessment score then determines the applicability of EDD requirements.
- (c) The Company, at a minimum, uses the following factors in its risk assessment methodology for calculating a customer's risk assessment score:
 - (i) Country/Location Risk;
 - (ii) Politically Exposed Person ("PEP") Risk;
 - (iii) Negative news/adverse media risk; and
 - (iv) Customer type/ownership structure risk.
- (d) In any of the following cases, the customer's risk assessment score will be automatically set to High:
 - (i) PEP, including immediate family member of close associate of such an individual;
 - (ii) Business relationships with customers and/or UBOs who are nationals of a "Sanctioned"⁶ Jurisdictions.

5.4 ENHANCED DUE DILIGENCE

- (a) The amount and type of information obtained in respect of new and existing customers, and the extent to which it is verified, must be increased where the perceived risk associated with the business relationship is higher.
- (b) Customers that pose higher ML/TF risks are subjected to enhanced scrutiny, or EDD.
- (c) The appropriate level of EDD required is based upon the results of the CDD that has been completed and risk rating generated by the risk scoring process.
- (d) Where the risks of ML/TF are assessed to be medium or high, the following EDD measures may be adopted:
 - (i) Obtaining additional customer information, such as occupation and further background searches on the customer, and, if applicable, its UBOs, controlling persons or related parties;

⁶ Refers to the following comprehensively sanctioned countries and regions: Cuba, Iran, North Korea, Syria and the following regions of Ukraine, Crimea, Donetsk and Luhansk.

- (ii) Carrying out additional searches (e.g. internet searches using independent and open sources to better inform the customer risk profile);
- (iii) Conducting additional customer name screening against adverse media/negative news databases;
- (iv) Where appropriate, undertaking further verification procedures on the customer, or UBOs or other person(s) within a legal person's structure, to better understand the risk of the customer;
- (v) Seeking and verifying additional information from the customer about the purpose and intended nature of a transaction or the business relationship;
- (vi) Obtaining additional information about the customer's SOW or SOF, this includes determining whether the customer's spending pattern matches his SOW and SOF;
- (vii) Increasing the frequency and intensity of customer periodic reviews and transaction monitoring; and
- (viii) Obtaining approval from senior management to continue the business relationship.

5.5 SIMPLIFIED DUE DILIGENCE

- (a) Where the risks of ML/TF are assessed by the Company as low, the Company may conduct SDD measures, which take the nature of the lower risk into account.
- (b) SDD measures will never be applied in situations that have been assessed as posing a higher ML/TF risk to the Company or in situations where there is a potential suspicion of ML/TF.
- (c) Where the risks of ML/TF are assessed to be low, the following SDD measures may be adopted:
 - (i) Limiting identification to the first three personal details set out in 4.1(a)(i)(1);
 - (ii) Verifying the identity of the customer and, if applicable, the UBO, after the establishment of the business relationship;
 - (iii) Adapting verification to be commensurate to the perceived lower risks (e.g. in a low risk situation, the Company may use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity);
 - (iv) Limiting the extent of personal details to be verified, as long as the Company is comfortable that it knows who the customer is;
 - (v) Reducing the frequency of customer periodic review; and
 - (vi) Reducing the degree of ongoing monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

5.6 BUSINESS RELATIONSHIPS WITH PEPs

- (a) Business relationships with PEPs may represent increased risks due to the possibility that individuals holding such positions may misuse their power and influence for personal gain or advantage, or for the personal gain and advantages of relatives and close associates. Such individuals may also use relatives or close associates to conceal funds or assets that have been misappropriated as a result of abuse of their official position or resulting from bribery and corruption.
- (b) PEP Definition:
 - (i) A PEP is defined as a Person who is, or has been entrusted with, prominent public functions and the direct family members or close associates of such persons. PEPs are also persons who are or have been entrusted with a prominent function by an international organization (i.e. World Health Organisation, UN, etc.) as members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions and the first family members or close associates of such persons.
 - (ii) It is important to note that both local PEPs (i.e. individuals entrusted with a prominent public function within Curacao) and foreign PEPs (i.e. individuals entrusted with a prominent public function outside of Curacao) are covered by this definition.
- (c) The Company screens for PEPs at onboarding and on an ongoing basis.
- (d) The Company will automatically classify all PEPs as high risk, which will subject them to EDD requirements and will only continue a business relationship with a PEP after obtaining approval from a Senior Manager and the CO (or their delegate).
 - (i) Although stricter due diligence is required for each PEP, this does not have to be the same for every PEP and is tailored for the risk of the PEP. To determine the level of EDD, the following is taken into consideration:
 - (1) The type of public function;
 - (2) The country from which the PEP originates; and
 - (3) The transactions that the PEP carries out.

5.7 PROHIBITED RELATIONSHIPS

- (a) Relationships with the following customers are prohibited ("Prohibited Customer"):
 - (i) Individuals, entities or governments subject to:
 - (1) Sanctions imposed by Curacao under the Sanctions National Ordinance and Kingdom Sanction Act;

- (2) Sanctions imposed by the UN;
- (3) Sanctions imposed by the EU; and
- (4) Sanctions imposed by OFAC in the US.
- (ii) Individuals or entities included in any internal blacklists;
- (iii) Individuals or entities seeking to maintain an account in an obviously fictitious name;
- (iv) Individuals or entities who fail to adequately complete KYC/CDD and, where applicable, EDD measures;
- (v) Individuals or entities where the Company knows or must assume that they finance terrorism or is a criminal organisation, or are part of or support such organizations;
- (vi) Banks that have no physical presence in their place of incorporation unless they are part of an appropriately supervised, consolidated financial group (i.e. shell bank);
- (vii) Individuals who are resident of a “Sanctioned”⁷ or “Restricted”⁸ Jurisdiction;
- (viii) Entities that are incorporated or legally registered in a “Restricted” or “Sanctioned” Jurisdiction;
- (ix) Entities where there is a UBO, Director/Connected Person or Authorised Person who is a resident of a “Sanctioned” Jurisdiction; and
- (x) Entities where there is a UBO, Director/Connected Person or Authorised Person who is resident of a “Restricted” Jurisdiction, and they are not able to provide reasonable evidence that all betting activity in relation to their account (apart from strictly back office functions) are being conducted outside of the “Restricted” Jurisdiction.

5.8 INTERNET PROTOCOL (“IP”) GEOFENCING

- (a) IP Geofencing is a security measure that restricts IP availability by geography, regardless of a customer’s access permission. In other words it is a virtual perimeter around a given location.
- (b) The Company utilizes this technology to block customer access to the website, and also to block registration, where a user is noted to have an IP that is geolocated to a “Sanctioned”⁹ or “Restricted”¹⁰ jurisdiction. This acts as a first level defence to block customers trying to access and register for an account on the Cloudbet Platform from “Sanctioned” or “Restricted” jurisdictions.

⁷ Refers to the following comprehensively sanctioned countries and regions: Cuba, Iran, North Korea, Syria and the following regions of Ukraine, Crimea, Donetsk and Luhansk.

⁸ As defined in the Terms of Service (<https://www.cloudbet.com/en/help/terms>).

⁹ Refers to the following comprehensively sanctioned countries and regions: Cuba, Iran, North Korea, Syria and the following regions of Ukraine, Crimea, Donetsk and Luhansk.

¹⁰ As defined in the Terms of Service (<https://www.cloudbet.com/en/help/terms>).

SECTION 6. ONGOING MONITORING OF CUSTOMER RELATIONSHIPS

6.1 ONGOING MONITORING INTRODUCTION

Once the customer has completed KYC/CDD and, where applicable, EDD, the Company will continue to monitor the customer, to ensure that their activity is consistent with expectations and to ensure that due diligence information/documentation remains up to date. The frequency and nature of the monitoring processes will depend upon the type of customer, the business undertaken, and the risk rating assigned to the customer.

6.2 PERIODIC REVIEWS

- (a) A periodic review is the scheduled review of a customer's due diligence file to ensure that the existing information and documentation on record is complete, up-to-date, adequate and relevant. This includes reviewing that the customer's risk assessment score is appropriate and, if needed, collecting updated or further documentation from the customer.
- (b) The frequency of the review is determined by the risk assessment score of the customer, with high risk customers undergoing an increased degree and frequency of monitoring, compared with medium and low risk customers who pose a lower ML/TF risk to the Company.

6.3 TRIGGER EVENT REVIEWS

- (a) When there is a material change to the customer, the event will trigger a review of the customer's due diligence file to ensure that the existing information and documentation on record is complete, up-to-date, adequate and relevant. This includes reviewing that the customer's risk assessment score is appropriate and, if needed, collecting updated or further documentation from the customer.
- (b) Examples of potential trigger events may include the following:
 - (i) A significant transaction or change in the way the customer's account is operated, including transactions that are unusual, suspicious, or not in line with the Company's knowledge of the customer;
 - (ii) A change to the customer's ownership/control structure;
 - (iii) A change to the authorised person(s) of the customer's account;
 - (iv) A significant change to the customers operating/business model; and
 - (v) A significant event or news articles related to the customer.

6.4 ONGOING SCREENING

- (a) Customer screening is conducted on an ongoing basis to ensure that all existing customers are periodically screened against the following lists:
 - (i) Relevant Sanctions Lists:

- (1) Sanctions imposed by Curacao under the Sanctions National Ordinance and Kingdom Sanction Act;
 - (2) Sanctions imposed by the UN;
 - (3) Sanctions imposed by the EU; and
 - (4) Sanctions imposed by OFAC in the US.
- (ii) PEP Lists; and
 - (iii) Relevant Law Enforcement Lists.
- (b) All lists are maintained by a third party service provider and are updated in accordance with the SLA that has been executed with them.
 - (c) Level 1 review of the alerts is conducted by the Customer Support Team, with Level 2 reviews handled by the CO.

6.5 IP GEOFENCING

- (a) The IP Geofencing controls mentioned previously in Section 5.8 also apply to existing customers on an ongoing basis. Where an existing customer is noted to be using an IP address geolocated to a “Sanctioned”¹¹ or “Restricted”¹² jurisdiction they will not be able to access their account and place bets.

6.6 OTHER CONTROLS

- (a) Playthrough requirement:
 - (i) A playthrough requirement is how many times a customer has to bet the funds that they have deposited before they can withdraw it.
 - (ii) The Company has implemented a 100% or 1x playthrough requirement on deposited funds from “non-KYC’ed” customers (i.e. if a customer deposits USD100, they will have to bet that amount before they are able to withdraw their funds).
 - (iii) This control helps the Company ensure that “non-KYC’ed” customers who are depositing funds on the platform do so with the intention to use the funds for wagering and makes it more difficult to use the platform as a quasi-crypto mixing service.

¹¹ Refers to the following comprehensively sanctioned countries and regions: Cuba, Iran, North Korea, Syria and the following regions of Ukraine, Crimea, Donetsk and Luhansk.

¹² As defined in the Terms of Service (<https://www.cloudbet.com/en/help/terms>).

SECTION 7. BLOCKCHAIN ANALYTICS AND TRANSACTION MONITORING

7.1 TRANSACTION MONITORING

- (a) Transaction Monitoring is a key feature of the Company's AML/CFT program and is overseen by the CO.
- (b) A risk-based approach is used to examine transaction and betting activity, with the Company monitoring on an ongoing basis, the activity of its customers by:
 - (i) Monitoring the activities of the customer to ensure that they are consistent with the nature of the business, the risk profile, and the source of wealth;
 - (ii) Identifying transactions, or patterns of transactions, that are complex, large, or unusual that have no apparent economic or lawful purpose and which may indicate ML/TF; and
 - (iii) Identifying an unusual change in the basis of the business relationship with the customer over time.
- (c) Any alerts are reviewed by the CO.

7.2 BLOCKCHAIN ANALYTICS SCREENING

- (a) Blockchain analytics screening is another key feature of the Company's AML/CFT program and is overseen by the CO. The Company utilizes a third party blockchain analytics screening tool to screen all cryptocurrency deposits and withdrawal transactions into and out of the Halcyon's wallet infrastructure. This allows the Company to detect transactional activity to or from risky service categories, such as sanctioned entities, terrorist financing and child abuse material.
- (b) Alerts are given a risk score based on counterparty risk exposure, the transaction amount and whether the transaction exhibits direct or indirect exposure.
- (c) Any alerts are reviewed by the CO.

7.3 MANUAL ESCALATIONS

- (a) At times the Company's employees may come across activity or behavior that could be considered as unusual and not consistent with expectations, and therefore potentially indicative of money laundering or other illicit activities. All employees are required to escalate such potentially unusual activity internally to the CO in writing (including supporting documentation) without delay.
- (b) All employees are trained annually to ensure they are aware of their responsibility in this regard.
- (c) Manual escalations may be escalated to the CO from the following sources:
 - (i) Employee escalations;
 - (ii) Third party service providers and partner escalations;
 - (iii) Receipt of regulatory or law enforcement enquiries or orders;
 - (iv) Escalations from the KYC/CDD, EDD or Name Screening processes;
 - (v) Customer complaints; and
 - (vi) External news or events.

SECTION 8. INVESTIGATION OF UNUSUAL ACTIVITY AND UTR FILING

8.1 INTERNAL ESCALATIONS OF POTENTIALLY UNUSUAL TRANSACTIONS

- (a) Potentially unusual or suspicious activity has to be reported to the CO. The CO has primary responsibility for the review and investigation of escalated matters, as well as the preparation and filing of UTRs with the FIU.
- (b) Potentially unusual or suspicious activity may be raised to the CO from a variety of sources, including, but not limited to the following:
 - (i) Automated/Manual monitoring and surveillance tools;
 - (ii) Employee escalations;
 - (iii) Receipt of regulatory or law enforcement enquiries or orders;
 - (iv) Escalation from the KYC/CDD, EDD or name screening processes;
 - (v) Customer complaints; and
 - (vi) External news or events.
- (c) When a matter is escalated to the CO, for a determination of whether there are reasonable grounds to suspect that the activity originates from criminal conduct, the CO reviews the facts and evidence in coming to a conclusion. The review and determination must be made in a timely manner. The decision of the CO must be well documented and stored appropriately. If the decision was to not file a UTR with the FIU, the reasoning for not reporting must be documented in a comprehensible manner (i.e. stating how the suspicion was eliminated and not just stating the decision).

8.2 DETERMINATION OF UNUSUAL TRANSACTIONS

- (a) When reviewing cases of suspected unusual activity, the CO will use their own judgement to determine whether a UTR should be filed with the FIU based on the fact that the activity is presumed, or there is cause to presume, that it is ML/TF related. However, Curacao regulation also requires the CO to file a UTR where the following activity is noted:
 - (i) Transactions that are reported to the police or the judicial authorities in connection with money laundering or the financing of terrorism;
 - (ii) Transactions by or for the benefit of any natural person, legal person, group or entity, whose name appears on a list that has been drawn up pursuant to the Sanctions National Ordinance;
 - (iii) Transactions of the value of NAf 5,000 or more (approximately USD 2,800)), regardless of the method of payment, be it cash, by check or other form of payment, or electronically or by another non-physical way. This includes, but is not limited to:
 - (1) A transfer from the eWallet or bank account of the Company to a local or international bank account or eWallet at the request of a customer;

- (2) Taking funds in deposit or releasing funds held in deposit at the request of a customer;
- (3) Selling tokens (which includes chips and credits) to a customer; and
- (4) Pay-out of prize money.

Note: A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAF 5,000 (approximately USD 2,800) or more and is considered per day.

8.3 FILING A UTR

- (a) Where the CO decides that a transaction/attempted transaction, or series of transactions/attempted transactions, is unusual and a UTR should be filed with the FIU, the CO will prepare a UTR for external reporting to the FIU without delay.
- (b) The Company has registered with the FIU and obtained access to the goAML reporting portal. The CO shall report to the FIU the details of the transactions by means of the goAML reporting portal. The CO shall ensure that all relevant fields are completed, including the core reason for suspicion and all information that the Company has about the transaction(s)/attempted transaction(s).

8.4 PROHIBITION OF DISCLOSURE / TIPPING OFF

- (a) It is a criminal offence for any person to disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU, without lawful authority or reasonable excuse. This is commonly known as the prohibition of “tipping off”. The reason for this is not to jeopardize an analysis or investigation into ML/TF.
- (b) The Company and its employees will never disclose this type of information to its customers nor to any third parties.
- (c) All employees are trained annually to ensure they are aware of their responsibility in this regard.
- (d) The only permitted exceptions, apart from disclosure to the FIU, are disclosures to:
 - (i) An officer or employee or agent of the Company for any purposes connected with the performance of that person’s duties;
 - (ii) A legal practitioner, attorney, or legal adviser, for the purposes of obtaining legal advice or representation in relation to the matter; and
 - (iii) The supervisory authority of the Company for the purposes of carrying out the supervisory authority’s functions.

8.5 POST-UTR FILING PROCEDURES

- (a) Once a UTR has been filed with the FIU, the Company will increase on-going monitoring on the account by designating the customer as high risk and submit additional reports to the FIU on any other suspected instances of ML/TF.

- (b) The Company will be cautious when it takes action to terminate a relationship or otherwise block additional transactions following reporting to the FIU. Drastic action shall only be taken when it is needed.
- (c) Where a business relationship has been assessed by the Company to be outside its AML/CFT risk tolerance, the relationship will be terminated and the customer offboarded. Where this is no reason for the retention of funds, the funds will be returned to the Customer as part of the offboarding process.
- (d) The Company may not terminate a business relationship if there are indicators that official measures are to be taken to seize the funds in question or the CO believes that the Company has appropriate controls in place to mitigate the risks posed by the customer.

SECTION 9. MANAGEMENT INFORMATION AND EXTERNAL REPORTING

- (a) The CO ensures that the Company has appropriate internal management information that allows them to assess and monitor the effectiveness of the AML/CFT controls in place and that appropriate reporting about the AML/CFT program is provided to:
 - (i) Senior management and the Board (on a periodic basis to allow them to understand and assess the status of the AML/CFT program); and
 - (ii) External Authorities (as per reporting requirements and other situations as appropriate, such as in instances where there is a significant AML/CFT event related to the Company).

SECTION 10. EMPLOYEE SCREENING

- (a) As part of onboarding as an employee of the Company, the new hire must provide a valid passport or other suitable identification document. Furthermore, the Company conducts sanction and criminal record checks to determine the person's honesty, integrity and reputation.
- (b) The Company will also ensure that sanction name screening of the new hire is conducted against the following lists:
 - (i) Relevant Sanctions Lists:
 - (1) Sanctions imposed by Curacao under the Sanctions National Ordinance and Kingdom Sanction Act;
 - (2) Sanctions imposed by the UN;
 - (3) Sanctions imposed by the EU; and
 - (4) Sanctions imposed by OFAC in the US.
 - (ii) Any alerts will be reviewed by the CO.
 - (iii) The Company will not employ anyone that returns a true positive hit as part of sanction screening.
- (c) Any potentially unusual or suspicious activity related to the Company's employees should be escalated to the CO as soon as reasonably practicable.

SECTION 11. RECORD KEEPING

- (a) The Company maintains customer, transaction and other records under this Policy that are necessary and required to meet the Company's AML/CFT obligations under applicable laws and regulations.
- (b) The Company maintains, for at least five years, all records on transactions to enable it to comply with information requests from competent authorities. Such records are sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.
- (c) Furthermore, the Company maintains all records obtained through the KYC/CDD and EDD process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended or after the date of the occasional transaction.
- (d) The KYC/CDD and EDD information, as well as the transaction records are made available to domestic competent authorities based upon appropriate legal authority.

SECTION 12. TRAINING

- (a) All the Company's employees are expected to be fully aware of the Company's AML/CFT Policy.
- (b) Every employee shall read and comply with this Policy.
- (c) The Company ensures that its employees receive mandatory training at regular intervals.
- (d) All training records and attendance lists shall be documented and kept for not less than 5 years for audit purposes.
- (e) The training includes but is not limited to:
 - (i) AML/CFT and Sanctions legislation and individual's roles and responsibilities;
 - (ii) KYC/CDD and EDD requirements for identifying and verifying customers;
 - (iii) What are ML/TF red flags to look out for in relation to potential unusual transactions or activity;
 - (iv) The ML/TF risks in the Company's business model;
 - (v) Prevailing techniques, methods and trends in ML/TF typologies as they relate to the gaming sector;
 - (vi) Manual escalation procedures; and
 - (vii) Prohibition of disclosure/"tipping off".
- (f) All new hires will be provided access to the Company's AML/CFT Policy as part of the new employee orientation along with the required new joiner training.
- (g) In addition to the general training for all employees, more targeted and tailored training will be given to employees depending on their job roles.

SECTION 13. QUALITY ASSURANCE (“QA”), COMPLIANCE TESTING AND INDEPENDENT AUDIT

13.1 QA AND COMPLIANCE TESTING

- (a) The CO will undertake:
 - (i) Regular spot checks of customer KYC/CDD and EDD files and transaction investigations to ensure compliance with AML/CFT policy requirements, and maintain records of such checks; and
 - (ii) An annual review in relation to the effectiveness of the AML/CFT program and provide a report to senior management and the Board.
- (b) The results of the annual review and most recent institutional risk assessments, amongst other things, will inform the CO whether any additional QA or Compliance Testing needs to be conducted on specific areas of the AML/CFT program.

13.2 INDEPENDENT AUDIT

- (a) The Company will, at least annually, commission an independent review of the AML/CFT program, which will, amongst other things, review the Company’s compliance with and the effectiveness of business, operations and compliance controls as they relate to AML/CFT.
- (b) Such independent review may be conducted either by an independent third party with relevant experience or by an internal audit function.
- (c) The independent review will cover at least the following areas:
 - (i) An evaluation of the Company’s AML/CFT Policies and Procedures;
 - (ii) Sample review of customer files;
 - (iii) Compliance management;
 - (iv) Performance of transaction testing;
 - (v) Assessment of training materials;
 - (vi) Assessment of compliance with applicable laws and regulations;
 - (vii) Evaluation of the transaction monitoring and screening system’s ability to identify unusual activity;
 - (viii) Interviews with employees and their supervisors who handle transactions;
 - (ix) Sample review of usual transactions on and beyond threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
 - (x) Assessment of the adequacy of the record retention system.
- (d) Results of any independent review will be reported to senior management and the Board in a timely manner. The Company will take prompt action to rectify any noted deficiencies and will ensure that all corrective actions have a corresponding deadline for completion.

13.3 EXAMINATIONS BY THE GCB

- (a) The GCB may as part of its supervisory role perform an examination of the Company to ensure that it is doing business in compliance with the applicable laws and regulations.
- (b) During such examinations, the Company will make available to the GCB such as information as the GCB may reasonably request, including:
 - (i) Its written and approved AML/CFT and Sanctions Policy;
 - (ii) Records of the Company's Institutional Risk Assessment;
 - (iii) The name of the CO responsible for the Company's overall AML/CFT policies and procedures and their designated job description;
 - (iv) Records of reported unusual transactions;
 - (v) Records of unusual transactions;
 - (vi) Records of unusual transactions which required closer investigations;
 - (vii) Records of frozen accounts;
 - (viii) Schedule of the training provided to the Company's personnel regarding AML/CFT;
 - (ix) The assessment report on the Company's policies and procedures on AML/CFT by the internal audit department or an external auditor; and
 - (x) The customer's files, including customer risk assessment, CDD, customer acceptance and transaction information.

APPENDIX 1. DEFINITIONS

(a) The following terms shall have the following meaning:

- (i) “AML” means Anti-Money Laundering;
- (ii) “AML/CFT Regulations” means the Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction issued by the Curacao GCB;
- (iii) “Authorised Person” means an individual authorised to act on behalf of a legal entity;
- (iv) “Board” means Halcyon’s Board of Directors and “Board Members” shall be construed accordingly;
- (v) “CDD” means Customer Due Diligence;
- (vi) “CFT” means Counter Financing Terrorism;
- (vii) “CO” means the formally designated Compliance Officer of the Company;
- (viii) “Company” means Halcyon Super Holdings BV, and “Halcyon” shall have the same meaning;
- (ix) “CPF” means Combatting Proliferation Financing;
- (x) “Cryptocurrency / Cryptocoin / Crypto / Digital Asset / DA / Digital Currency / Virtual Asset / Virtual Currency” means a digital representation of value that can be digitally traded and functions as (1) a medium of exchange, and/or (2) a unit of account, and/or (3) a store of value, but does not have legal tender status (i.e. when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction and fulfills the above functions only by agreement within the community of users of the cryptocurrency;
- (xi) “Directors” means directors appointed to the Board and “Director” shall mean any of them;
- (xii) “EDD” means Enhanced Due Diligence;
- (xiii) “EU” means the European Union;
- (xiv) “FATF” means Financial Action Task Force;
- (xv) “FATF Guidelines” means the FATF Guidance for Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers / FATF Guidance on the Risk-Based Approach for Casinos;
- (xvi) “Fiat Currency / Real Currency / Real Money / National Currency” means the coin and paper money of a country that is designated as its legal tender, circulates, and is customarily used and accepted as a medium of exchange in the issuing country;
- (xvii) “FIU” means the Curacao Financial Intelligence Unit, unless otherwise stated;
- (xviii) “GCB” means the Curacao Gaming Control Board;
- (xix) “IP” means Internet Protocol;

- (xx) “KYC” means Know Your Customer;
- (xxi) “MI” means management information and is used in the context of periodic reporting to senior management;
- (xxii) “ML” means money laundering and is defined in Section 2;
- (xxiii) “NOIS” means the Curacao National Ordinance on identification when rendering services;
- (xxiv) “NORUT” means the Curacao National Ordinance reporting unusual transactions;
- (xxv) “OFAC” means the US Office of Foreign Asset Control;
- (xxvi) “PEP” means politically exposed person and is defined in Section 5.6;
- (xxvii) “PF” means proliferation financing and is defined in Section 2;
- (xxviii) “Policy” means this AML/CFT and Sanctions Policy;
- (xxix) “Prohibited Customer” means a customer that is listed in Section 5.7;
- (xxx) “QA” means quality assurance;
- (xxxi) “RBA” means risk based approach and is defined in Section 3;
- (xxxii) “SDD” means simplified due diligence;
- (xxxiii) “SLA” means service level agreement;
- (xxxiv) “SOF” means source of funds;
- (xxxv) “SOW” means source of wealth;
- (xxxvi) “TF” means terrorist financing and is defined in Section 2;
- (xxxvii) “UBO” means Ultimate Beneficial Owner and is defined in Section 5.1(a)(i)(2)(i);
- (xxxviii) “UN” means the United Nations;
- (xxxix) “US” means the United States of America; and
- (xl) “UTR” means unusual transaction report.

Halcyon_AML_Policy_v3.0 (FINAL)

Final Audit Report

2025-04-10

Created:	2025-04-09
By:	Andy Meiers (andy@bgl.sc)
Status:	Signed
Transaction ID:	CBJCHBCAABAANcVbx-a0XVJBH6enhEQvk6YGDtKWYM_T

"Halcyon_AML_Policy_v3.0 (FINAL)" History

-  Document created by Andy Meiers (andy@bgl.sc)
2025-04-09 - 3:39:23 AM GMT
-  Document emailed to peter.m@churchillhk.co for signature
2025-04-09 - 3:39:47 AM GMT
-  Email viewed by peter.m@churchillhk.co
2025-04-10 - 5:37:37 AM GMT
-  Signer peter.m@churchillhk.co entered name at signing as P. Manktelow
2025-04-10 - 5:38:14 AM GMT
-  Document e-signed by P. Manktelow (peter.m@churchillhk.co)
Signature Date: 2025-04-10 - 5:38:16 AM GMT - Time Source: server
-  Agreement completed.
2025-04-10 - 5:38:16 AM GMT