

Mead Software Technologies B.V.

Anti Money Laundering & Terrorist Financing Manual

Document Status

Custodian: Compliance Officer

Date: June 2025

Issue	Date	Revision Summary
1.1	Jun 2025	For Issue
<i>UNCONTROLLED WHEN PRINTED</i>		

Notes:

1. Hard copies of the Document previous to the latest version must be destroyed.
2. The Compliance Officer can supply a hard copy of the controlled version.
3. Any question or comments regarding the Document should be directed to the Compliance Officer.
4. Significant changes to the Document in subsequent versions shall be highlighted in blue text.

Table of contents

Document Status	1
Definitions	3
Section 1	6
1.1. Introduction.....	6
1.2. Money Laundering Compliance Staffing	6
Section 2	7
2.1 Risk Assessment.....	7
2.1.1. Business Risk Assessment.	7
2. 1. 2. Risk Assessment of Participants and Business Participants.....	7
2. 1. 3. Higher Risk Participants	8
2. 1. 4. Technological Developments	8
Section 3	8
3.1 Customer Due Diligence -Requirement of Licensee's.....	8
3.1.1. Customer Due Diligence.....	8
3.1.2. Enhanced Customer Due Diligence.....	10
3.1.3. Timing of identification and verification.	10
3.1.4. Non-compliance with customer due diligence measures.	11
Section 4	12
4.1 Ensuring Compliance and Record Keeping.....	12
4.1.1. Record-keeping.	12
Section 5	13
5.1 Compliance Culture	13
5.1.1. Staff Integrity and Positive AML/CFT Culture.....	13
5.1.2. Staff Training	13
Section 6	14
6.1 Miscellaneous	14

Definitions

The following definitions apply throughout this document, unless context otherwise requires

"B2C Operators" means the companies which license M-CAP from MST and hold the relevant B2C gaming license

"Business Participants" means a person participating, in the course of business, in online gambling other than a licence holder

"CGA" means the Curacao Gaming Authority

"Customer Due Diligence Information" means-

- (a) identification data, and
- (b) any other files and correspondence relating to the customer relationship;

"Customer Due Diligence Measures" means-

- (a) identifying the customer and verifying the customer's identity on the basis of identification data,
- (b) identifying, where there is a beneficial owner or underlying principal who is not the customer, the beneficial owner or underlying principal and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the licensee is satisfied that it knows who the beneficial owner or underlying principal is, including, in the case of a legal person, trust or other legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement,
- (c) identifying any person purporting to act on behalf of a customer and verifying that identity on the basis of identification data and the authority of the person so acting, and
- (d) obtaining information in the purpose and intended nature of the customer relationship;

"Codes" means those implemented by the Curacao Gaming Authority

"Document" includes information recorded in any form (including, without limitation, in electronic form);

"Enhanced Due Diligence" means where a customer's risk rating is determined to be higher than normal, additional identification and verification steps are required to the normal customer due diligence measures, these including taking the following steps-

- (a) consider whether additional identification data needs to be obtained;
- (b) consider whether additional aspects of the participant's identity or the identity of the business participant need to be verified;
- (c) take reasonable measures to establish the source of any funds and of the wealth of the participant and any beneficial owner and underlying principal; and
- (d) consider what on-going monitoring should be carried on in accordance with the Codes

"FATF Recommendations" means the Financial Action Task Force Recommendations on Money Laundering and the Financial Action Task Force Special Recommendations on Terrorist Financing as revised or reissued from time to time;

"Guidance Notes" means the Curacao Gaming Authority Guidance notes for AML-CFT

“High Risk Relationship” means a customer relationship which has a high risk of involving money laundering or terrorist financing or fraud and related terms shall be construed accordingly;

“Identification Data” means documents, data or information relating to identification which are from a reliable and independent source;

“MLRO” means Money Laundering Reporting Officer

“Money Laundering” means the process by which criminal or ‘dirty’ money is legitimised or made ‘clean’, including any action taken to conceal, arrange, use or possess the proceeds of any criminal conduct.

“MST or Company” means Mead Software Technologies B.V.

“M-CAP” means the MST Content Aggregation Platform.

“PEP or Politically Exposed Person” means any of the following resident in a country or territory -

- (a) A natural person who is or has been entrusted with prominent public functions, including -
 - (i) a head of state, head of government, minister or deputy or assistant minister;
 - (ii) a senior government official;
 - (iii) a member of parliament;
 - (iv) a senior politician;
 - (v) an important political party official;
 - (vi) a senior judicial official;
 - (vii) a member of a court of auditors or the board of a central bank;
 - (viii) an ambassador, chargé d’affaires or other high-ranking officer in a diplomatic service;
 - (ix) a high-ranking officer in an armed force;
 - (x) a senior member of an administrative, management or supervisory body of a State-owned enterprise;
 - (xi) a senior official of an international entity or organisation; and
 - (xii) an honorary consul;
- (b) any of the following family members of a person mentioned in sub-paragraph (a)
 - (i) a spouse;
 - (ii) a partner considered by national law as equivalent to a spouse;
 - (iii) a child;
 - (iv) the spouse or partner of a child;
 - (v) a sibling;
 - (vi) a parent;
 - (vii) a parent-in-law;
 - (viii) a grandparent; or
 - (ix) a grandchild;
- (c) any close associate of a person mentioned in sub-paragraph (a), including —
 - (i) any natural person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with such a person;
 - (ii) any natural person who has sole beneficial ownership of a legal entity or legal

arrangement that is known to have been set up for the benefit of such a person;
(iii) any natural person who is in a position to conduct substantial financial transactions on behalf of such a person.

“Regulatory Bodies” means

- (a) Council of European Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL for short)
- (b) Financial Action Task Force (FATF for short)
- (c) National Crime Agency (NCA for short)
- (d) Curacao Gaming Authority
- (e) Financial Intelligence Unit Curacao (FIU for short)

“Sanctioned Individual” means a person who is listed on the HM Treasury and Office of Financial Sanctions Implementation list.

“Transaction Document” means a document which is a record of a transaction carried out by an licensee with a registered customer and which, as a minimum, identifies the customer, the nature and date of the transaction and the type and amount of the currency involved;

Section 1

1.1.Introduction

MST is a software supplier which licenses M-CAP on a B2B basis to B2C Operators. The purpose of this document is to outline the necessary controls required to be undertaken by MST and its staff in order to forestall, prevent and detect customers attempting to carry out money laundering and terrorist financing activities through M-CAP. This also includes the requirements that MST places on its B2C Operators regarding the minimum AML/CFT measures which the B2C Operator must implement.

This document aims to address those requirements set out in the Guidance Notes issued by the CGA and Relevant Bodies.

The Company objectives regarding its AML/CFT Policy is as follows:

- Have a business in which the Company and its B2C Operators do not facilitate any money laundering or funding of terrorist activities
- Have processes, supported by the relevant staff training, which highlight and report any suspicious activities
- Create a workplace environment whereby staff are empowered to raise any concerns to the CO regarding any suspicious activities

This Document is intended to be distributed to all staff and shall be required to be adhered to by the Company and all 3rd Parties which have products that generate revenue on M-CAP, B2C Operators who use M-CAP and any advisors having any impact on this Document of Company policy.

As a minimum this Document shall be reviewed and approved annually by 31 December of each calendar year by the MST Board.

1.2.Money Laundering Compliance Staffing

MST has appointed a CO who acts as the MLRO to ensure all staff are made aware of the approved policies, controls and procedures put in place in order to forestall, prevent and detect customers attempting to carry out money laundering and terrorist financing activities on M-CAP. Any changes in the personnel occupying these roles will be disseminated across the company immediately.

The appointment of the CO/MLRO shall be signed off by the board and will also be disclosed to relevant regulatory bodies in order to provide a direct reporting line for disclosures of suspicious activities. The following bodies will be made aware of the appointments:

For MST:

- Curacao Gaming Authority

Section 2

2.1 Risk Assessment

2.1.1. Business Risk Assessment.

The business risk assessment aims to provide structured program to manage risks and encourage accountability while empowering teams with a channel to surface operational risks so that control deficiencies can be addressed. The management are required to provide an environment that supports robust control self-assessment aimed at 'self-detect/ self-heal', and build a risk management conscience into business-as-usual.

This conscience in turns supports operational stability with the foresight to mitigate weaknesses before they materialize as incidents with business impact.

The Business Risk Assessment is approved by the MST Board, updated at least annually and, as a minimum, includes considerations of the following:

- (a) The nature, scale and complexity of MST's activities;
- (b) The products and services we offer to customers;
- (c) Our customer base;
- (d) The manner in which our products and services are provided (e.g. via intermediaries);
- (e) Any reliance placed upon third parties for elements of CDD; and
- (f) Any technological development risks.

2. 1. 2. Risk Assessment of Participants and Business Participants

The Company maintains a risk assessment policy as outline in 2.1.1 above and shall be used to estimate the level of risk related to money laundering and the financing of terrorism from participants or Business Participants it intends to contract with. This Customer Risk Assessment shall be approved by the MST Board and is reviews/updated at least annually.

The assessment shall take into regard the following factors when determining the risk level:

- (a) the value of funds deposited with the company;
- (b) the jurisdiction of participant or business participant;
- (c) the source of funds deposited;
- (d) any other relevant matter brought to the attention of the company during the account opening process for the participant or the business participant;
- (e) any relevant supervisory or regulatory guidance given by the Isle of Man Gambling Supervision Commission;
- (f) the legal nature of the business participant.

2. 1. 3. Higher Risk Participants

Participants or business participants that pose a higher risk shall automatically undergo enhanced due diligence (EDD). These higher risk participants shall be determined in the Customer Risk Assessment outlined in 2.1.2 and shall include but not restricted to the following:

- (a) a politically exposed person;
- (b) a person, legal person or legal arrangement resident or located in a country that the company has reason to believe does not apply, or insufficiently applies, the FATF Recommendations; or
- (c) a person, legal person or legal arrangement that is the subject of any notices or warnings issued from time to time by the Isle of Man Gambling Supervision Commission or the UK Gambling Commission.

2. 1. 4. Technological Developments

The Company shall remain vigilant to technological developments in the field of online gambling, and ensure that it prevents the mis-use of such technology for the purposes of money laundering or the financing of terrorism. The company shall ensure that a risk assessment is carried out on any proposed development changes to the existing products on the site by using the business risk assessment policy outlined in 2.1.1 above.

New technologies may include but limited to the following:

- (a) Development of a new product;
- (b) A new delivery mechanism;
- (c) New business practice
- (d) New technology that used to deliver new or old services

Further, all companies associated with the introduction of new products or modification to the existing services that the company wishes to engage with shall undergo due diligence checks in order to determine the following:

- (a) the partner/supplier is who they claim to be;
- (b) is financially sound;
- (c) has the capacity, capability and expertise to deliver;
- (d) has the systems and process to deliver;
- (e) has a strong understanding of the contract deliverables and requirements and its obligations under the contract.

Section 3

3.1 Customer Due Diligence -Requirement of Licensee's

3.1.1. Customer Due Diligence.

In order to forestall, prevent and detect customers attempting to carry out money laundering and

terrorist financing activities the company ensures its Licensees maintain strict controls on carrying out customer due diligence in their B2C business. These required controls are outlined below:

KYC (Know Your Customer)

At first registration of a customer account, automated due diligence checks are carried out on customer supplied dated by the Sportsbook and Casino software prior to qualifying for deposits and payments. The following checks are carried out:

- To ensure that the customer is physically in the territory the business uses geolocation software to confirm via the Internet Protocol Address used by the customer.
- Automated group checking software is used to verify that the customer is :
 - of legal age to gamble;
 - has provided his or her correct name and address information.

Qualifying Payments

The Code requires that full evidence of identity is required when any payment exceeding **€2,000 or £ equivalent** is made to or by a customer.

Customer Due Diligence shall be carried on customers making the following deposits or withdrawals:

- (a) a deposit or withdrawal of **€2,000 or £ equivalent** or more, or
- (b) This can be a one-off payment, or when taken with all other payments made to or by the client within 30 days immediately preceding the date on which the payment is to be made, the aggregate amount exceeds **€2,000 or £ equivalent**.

The following Customer Due Diligence (CDD) checks shall be carried out in order to confirm the identity of the customer:

- (a) Proof of ID and address via documentation;
 - (b) Confirmation of contact email address via communication;
-
- If validated documents proving identity (ID) and proof of address (POA) are on file and less than 6 months old (date of receipt not date of the document), no action is required other than to monitor the account.
 - If no documents are on file or they are older than 6 months then a request must be sent to the customer requesting these documents and detailing what documents are applicable. Open source negative press/adverse media, social media checks **SOF** and checks should be commenced at this time. If the QP relates to a withdrawal, this must be held until the documents are received.
 - If no documents have been received within 7 days of contacting the customer, the account must be frozen.
 - Once documents have been received and they are validated, the account may be unfrozen if frozen and withdrawal processed.
 - If there is any suspicious activity associated with an account, Enhanced Due Diligence (EDD) procedures must be implemented.

The daily reports shall be monitored on the Sportsbook and Casino to detect any qualifying payments which should be raised to the Fraud and Risk team for further action as outline below.

Further, deposits limits can be automatically be set in the admin systems and any deposits exceeding this deposit level will be automatically red flagged for further investigation and identity verification.

The required documentation per deposit limit is outlined in the table in Appendix B.

3.1.2. Enhanced Customer Due Diligence.

Enhanced due diligence (EDD) shall be carried out by the Fraud and Risk team and CS teams in relation to the following customer relationships:

- (a) a relationship in which the customer or any beneficial owner or underlying principal is a politically exposed person (PEP) reference shall be made to the definition of a PEP noted in the definition section above;
- (b) a relationship where the customer is established or situated in a country or territory that does not apply or insufficiently applies the FATF Recommendations;
- (c) a relationship which has been assessed as a high risk relationship e.g. suspected of carrying out money laundering activity. [financing of terrorism or fraud](#).
- (d) A customer meets the high risk account threshold criteria when he or she deposits an amount of [€15,000 or £ equivalent](#) over any 30 day period and will automatically be considered as high risk and the EDD process initiated, similarly should he or she over the same time period stake an amount of or in excess of [€50,000 or £ equivalent](#) the EDD process will be initiated. (The stake total will be made up of deposit and sums staked including 'churn' or winnings).
- (e) [Should a customer from registration to current day deposit or withdraw a total of €50,000 or £ equivalent, known as a lifetime threshold, the EDD process will be initiated. If the customer has already been the subject of an EDD check, this threshold does not apply. However, at each following increment of the same sum \(e.g. at €100,000 and €150,000 etc.\) the same lifetime threshold check applies if other thresholds are not met beforehand.](#)

The following Enhanced Due Diligence checks shall be carried out in order to confirm the identity of the customer:

- (a) Proof of ID and address via documentation;
- (b) Confirmation of contact email address via communication;
- (c) Confirm source of funds and source of wealth;
- (d) Open source negative press/adverse media, social media checks.

If the customer trying to register is identified as a PEP, approval shall be sought from the MLRO on whether to register the customer, or, in the case of an existing registered customer, keeping the account open. The MLRO shall ensure a risk assessment is carried out on all PEPs.

3.1.3. Timing of identification and verification.

Verification is conducted immediately after the new account is created by a customer. The Customer support team shall request verification documents from the customer if the automated verification software flags that the information provided is incorrect. Only when these documents have been received and authenticated by the customer support team shall the customer be allowed to proceed with funding his account.

3.1.4. Non-compliance with customer due diligence measures.

Where a customer is unable to comply with the customer due diligence or the enhanced due diligence requirements the customer will not be allowed to register a funded account with the relevant site. In the case where the customer has an existing account and is being asked for non "stale" documents (less than 6 months since receipt and validation) and is unable to produce any authenticate documentation their balance shall be with returned to the customer and his account terminated. All reports of such instances shall be reported back to the MLRO or in their absence the NO who shall determine whether a disclosure to the relevant financial institution is necessary. All records of these cases shall be retained as outlined in section 4 below.

Section 4

4.1 Ensuring Compliance and Record Keeping

4.1.1. Record-keeping.

Record-keeping in respect of Customer identity/ Due diligence – all records, either paper or electronic files are retained in a secured location. User password protection is required for network files, locked filing cabinets for paper files. Keys for the cabinets are restricted to the relevant Senior Heads of department.

Records of transactions – All payment and withdrawal transactions are maintained securely in the Admin system and can be retrieved for viewing at any time.

Retention of Records – as a minimum, records shall be retained for a period of 6 years after a Customer ceases to be an active Customer on our sites. Any Customer under investigation due to possible fraudulent activities and who are undergoing investigation shall have their records retained until the relevant groups no longer requires the company to retain them.

Section 5

5.1 Compliance Culture

5.1.1. Staff Integrity and Positive AML/CFT Culture.

In order to satisfy the integrity of new hires the following information shall be obtained:

- Obtain and confirm references;
- Confirm employment history and the qualifications advised;
- Request details of any regulatory action taken against the individual (or the absence of such action); and
- Request details of any criminal convictions (or the absence of such convictions) and verify where possible.

Where relevant information has been requested but not obtained the type and reason for the missing information shall be documented and kept on file.

5.1.2. Staff Training

All staff shall be given training and refresher training at least twice a year on methods of detecting money laundering and terrorist financing activities. The training modules are designed and run by a dedicated training department in conjunction with third party experts and shall ensure staff are aware of:

- the provisions of the money laundering and terrorist financing requirements;
- their personal obligations under the money laundering and terrorist financing requirements;
- the internal reporting procedures;
- MST's policies and procedures to prevent money laundering and the financing of terrorism;
- MST's participant and business participant identification, verification, record-keeping and other procedures to prevent money laundering and the financing of terrorism;
- the recognition and handling of suspicious transactions;
- new developments, including information on current techniques, methods and trends in money laundering and the financing of terrorism.

Refresher training courses where possible will also be scheduled throughout the year to take into account new regulations and to raise employee's awareness. The Training Department shall ensure all details of the staff receiving training are recorded along with the dates that the training took part and any results of any test undertaken.

Section 6

6.1 Miscellaneous

Application to associates.

The company uses the services of Compliwise to ensure the compliance of this Document by both the Company and its Licensed Operators.