

To this end, the Company conducts periodic AML compliance audits, at least annually and additionally in the event of significant regulatory changes, operational developments, or material compliance breaches. These audits are carried out by qualified internal or external parties who are independent from daily compliance operations and who possess the requisite expertise in financial crime risk management.

The audit scope includes, but is not limited to:

- **Evaluation of Policies and Procedures** – Reviewing whether the AML/CTF/CPF framework is up to date, aligned with legal standards, and effectively applied across departments.
- **Effectiveness of Risk-Based Approach** – Testing the design and implementation of Business Risk Assessments (BRA), Customer Risk Assessments (CRA), and other relevant methodologies.
- **Transaction Monitoring and SAR/STR Filing** – Assessing the adequacy of transaction surveillance tools and the timeliness, quality, and completeness of suspicious activity reporting.
- **CDD and KYC/KYB Compliance** – Sampling client files to verify that due diligence procedures, beneficial ownership checks, and document retention policies are implemented correctly.
- **Sanctions Screening Controls** – Verifying the application and currency of screening mechanisms against relevant international and domestic sanctions lists.
- **Employee Screening and Training** – Assessing adherence to employee screening requirements and the effectiveness of ongoing AML training programs.
- **Technology Risk Controls** – Reviewing systems supporting AML compliance, including data integrity, automated risk scoring, and access rights.

The outcomes of the internal audits are formally documented in comprehensive reports, which are submitted directly to senior management and the Board of Directors, in accordance with CGA AML Regulation Section V.7. These reports identify any deficiencies or areas for improvement and include clear recommendations and timelines for remediation.

Furthermore, audit findings that reveal material weaknesses, breaches, or risks to AML/CTF/CPF compliance are escalated immediately to the Compliance Officer and the Board, with follow-up audits conducted to verify implementation of corrective actions.

Luckyroo N.V. maintains an audit trail and full documentation of all internal audit activities for a minimum of five (5) years and makes such records immediately available to the Curaçao Gaming Control Board (GCB) upon request. The Company is committed to transparency, accountability, and continuous improvement in its AML/CTF/CPF compliance framework.

17. Regulatory Access and Cooperation

Luckyroo N.V. fully acknowledges the supervisory and enforcement authority of the Curaçao Gaming Control Board (GCB) and commits to complete, proactive cooperation with all regulatory examinations and oversight activities. To this end, the company grants the GCB and any other legally empowered authority unrestricted, immediate, and comprehensive access to all data, systems, records, and personnel necessary for the assessment of its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) framework.

This includes, but is not limited to:

- Customer due diligence records
- Transaction histories and monitoring data
- Internal risk assessments
- Policies and procedures
- Communication logs and training materials
- Audit trails, reports, and logs
- Compliance-related systems and platforms

Access shall be granted for both on-site and remote inspections, including the right to request supplementary documentation, system walkthroughs, and clarifications. Luckyroo N.V. ensures that all required information is readily retrievable, promptly provided upon request, and securely maintained for a minimum of five (5) years, or longer where legally mandated. Furthermore, the company commits to full cooperation with any post-inspection findings, including corrective action plans and remedial steps as directed by the GCB.

18. Internal Audit and Reporting

Luckyroo N.V. shall establish and maintain an independent internal audit function for the purpose of evaluating the effectiveness, adequacy, and operational integrity of its Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CTF/CPF) framework. Internal AML audits shall be conducted at least annually, or at such greater frequency as may be necessitated by the Company's risk exposure, regulatory developments, or material changes to business operations. Audits shall be performed by the Internal Audit team, or by an independent third-party auditor where required to ensure full independence, objectivity, and professional competence.

The scope of each internal audit shall include, but shall not be limited to: the review and testing of AML/CTF/CPF policies and procedures; assessment of the effectiveness of transaction monitoring systems and sanctions-screening controls; verification of the adequacy and accuracy of Suspicious Activity Report (SAR) filings; evaluation of customer due diligence and enhanced due diligence practices; examination of training programs and training effectiveness; and testing of governance, oversight, and record-keeping arrangements. The audit shall also assess whether the Company's systems and controls remain proportionate to its risk profile and compliant with statutory and regulatory obligations.

All internal audit reports, supporting documentation, working papers, and remedial action logs shall be maintained in a secure and tamper-proof manner and retained for a minimum period of five (5) years, or longer where required by law or regulation. The internal audit function shall have unrestricted, unimpeded access to all systems, personnel, records, and information necessary to discharge its duties effectively and in full compliance with applicable regulatory expectations.

HOW TO USE THIS?		NEW Risk score		NEW Risk level		Understanding assessment		Last update date	
1. Only yellow and blue flags have to be filled. 2. Comment section is optional, however, it is not necessary for completion of this level. 3. Validity of questions has response list in question. Change answer(s) should be response.		0.00		Low					

Client no.	Name

Risk Category	Question	Risk score	Risk level	Additional comments
Others	Customer's Age			
Citizenship	Customer's Citizenship			
Citizenship	Customer's Second Citizenship			
Citizenship	Customer's Country of Birth			
Citizenship	Customer's Country of Residence			
Other	Does Customer have the status of REPUBLIC (Politically Exposed Person/Relative and Close Associate)?			
ACCOUNT PROFILE				
Other	Purpose of account registration?			
FUND SOURCE AND INCOME STATUS				
Other	Source of funds			
Other	Source of wealth			

This Policy is adopted to ensure full compliance with CGA AML Regulation V.4, which requires firms to implement adequate screening procedures for employees both prior to employment and on an ongoing basis.

The Company further adopts an Employee Screening Checklist, which forms an integral part of this Policy and must be completed in all cases as evidence of adherence to the screening requirements set out herein.

This Policy applies to:

- All full-time, part-time, temporary, and contract employees.
- Senior Management, the Compliance Officer and all staff involved in AML/CTF obligations.
- Individuals engaged through third-party or outsourced arrangements performing regulated or sensitive functions.

No individual may commence employment or assume duties in a sensitive role until all screening measures required under this Policy have been satisfactorily completed.

Requirements

Luckyroo N.V. shall ensure that all individuals are fit, proper, and suitable to perform their assigned duties. Screening procedures must be risk-based, proportionate to the sensitivity of the role, and documented.

The screening process consists of:

- (a) Pre-Employment Screening,
- (b) Fit-and-Proper Assessment (for designated roles),
- (c) Ongoing Screening, and
- (d) Completion of the Employee Screening Checklist.

Pre-Employment Screening

Human Resources ("HR"), in coordination with the Compliance Department, shall conduct the following mandatory pre-employment checks:

- Criminal Background Checks

A criminal record check shall be obtained to determine whether the applicant has been convicted of offenses relating to dishonesty, fraud, financial crime, money laundering, terrorist financing, or other conduct incompatible with the integrity expected of Company personnel.

- Verification of Identity

Applicants must present valid government-issued identification. HR shall verify identity authenticity and consistency.

- Verification of Academic and Professional Qualifications

All educational degrees, professional certifications, licenses, and other credentials relevant to the position must be independently verified.

- Employment History Verification

The Company shall confirm prior employment, roles, responsibilities, performance, and conduct, subject to applicable legal limitations.

- Reference Checks

At least two professional references must be obtained and documented. Adverse information must be escalated to Compliance for assessment.

Completion of the Employee Screening Checklist is mandatory before any offer of employment may be finalized.

Fit-and-Proper Assessment

A formal Fit-and-Proper Assessment shall be conducted to determine the individual's suitability for the role, evaluating the following:

- Integrity and Reputation

Absence of adverse regulatory findings, criminal convictions, ethical misconduct, or behaviour inconsistent with professional honesty.

- Competence and Professional Capability

Assessment of qualifications, technical skills, AML/CTF experience, and the capacity to discharge regulatory obligations.

- Financial Soundness

Where permitted by applicable law, consideration of financial history including bankruptcy, insolvency, or financial misconduct.

- Independence and Conflict of Interest

Assessment of the ability to act independently and without real or perceived conflicts of interest.

A Fit-and-Proper Assessment Form shall be completed, reviewed by the Compliance Department, and retained with the Employee Screening Checklist.

Ongoing Screening and Monitoring

Periodic Screening

Employees in sensitive, compliance-related, or high-risk roles shall undergo screening at least annually, including but not limited to:

- Updated criminal record checks (where legally permissible),
- Role suitability evaluations,
- Conduct and performance reviews,
- Confirmation of continued independence and absence of conflicts.

Trigger-Based Rescreening

Additional screening is required when:

- An employee is promoted or transferred to a sensitive role,

- Allegations or indicators of misconduct are identified,
- Regulatory or business changes increase the risk profile of the role,
- External information gives rise to concerns regarding fitness or propriety.

Continuous Conduct Monitoring

Supervisors and the Compliance Department must report any concerns regarding employee behavior or integrity for immediate assessment.

Mandatory Checklist Completion

For each periodic or trigger-based rescreening, the Employee Screening Checklist must be updated and retained.

Documentation and Record-Keeping

The Company shall maintain complete and accurate records of all screening activities, including:

- Background check reports,
- Verification evidence,
- Fit-and-Proper Assessments,
- Completed Employee Screening Checklists,
- Internal approvals and escalation notes,
- Any adverse findings and remedial actions taken.

Records shall be retained for not less than five (5) years, or longer where required by law or regulation, and shall be made available to competent authorities upon request.

Responsibilities

Human Resources

- Administers pre-employment screening and maintains screening files.
- Ensures completion of the Employee Screening Checklist.
- Escalates concerns to Compliance.

Compliance Officer

- Oversees screening for AML/CTF-related roles.
- Conducts Fit-and-Proper Assessments.
- Approves employment in sensitive roles.
- Ensures compliance with CGA Regulation V.4.

Senior Management

- Ensures adequate resources and oversight.
- Approves any exceptions or escalated cases.

- Reviews periodic compliance reports.
-

Compliance and Enforcement

Failure to comply with this Policy, including failure to complete the Employee Screening Checklist or Fit-and-Proper Assessment, may result in disciplinary action up to and including termination of employment.

The Company affirms that this Policy satisfies the requirements of CGA AML Regulation V.4 and shall review the Policy annually to ensure continued regulatory compliance.

New Employee check list

Employee: _____

Starting date: _____

1.	Copy of national Identity card or passport	€
2.	Work permit (if needed)	€
3.	Proof of Residence	€
4.	Certificate of clear criminal record	€
5.	Non-Bankruptcy letter	€
6.	Reference letter from previous employer	€
7.	License/certificates	€
8.	CV (Curriculum Vitae)	€
9.	Good repute questionnaire	€
10.	Diploma of high education	€
11.	AML and IOM acknowledgement letter	€
12.	Privacy Notice	€
13.	Induction & Initial Training Policy/Acknowledgement form	€
14.	Employment Agreement	€

Appendix III

Sanctions policy

Background

Luckyroo N.V. is obliged to comply with laws imposing financial and other restrictions on dealings with certain entities, individuals and countries. This Sanctions Policy (hereinafter the “Policy”) sets

out requirements and procedures designed to promote compliance with such laws (sanctions). Sanctions are a policy tool that national governments and multinational organisations use to constrain and deter perceived threats to their security, or to conform international conduct to recognised international standards. Sanctions arise in response to the conduct of countries, geopolitical rivals or transnational actors or trends. While national-level and multilateral sanctions regimes vary in content, rules, and restrictions, and the substance and frequency of enforcement action, they tend to fall into one of the below categories:

- **Comprehensive sanctions.** These sanctions target entire countries or geographic regions (e.g., the Crimea Region of the Ukraine) and prohibit most activity involving those countries or jurisdictions. Comprehensive sanctions aim to alter government behavior by imposing economy-wide costs, restricting access to arms and tools of internal repression, and restricting access to a wide range of goods and services.
- **Regime-based sanctions.** These sanctions target current (or former) governments or regimes. They are not comprehensive: although they are associated with particular countries, they are primarily list-based, focused on officials involved in activity deemed to be a threat to national security, economy, or foreign policy and on their associates. These sanctions tend to be paired with limited export controls or embargoes and related financing prohibitions. Most regime-based sanctions aim to protect human rights, combat state-sponsored or grand-scale corruption, and support democratic processes, institutions, and the rule of law.
- **Sectoral sanctions.** These sanctions target entities in a key sector or sectors of a country's economy. Importantly, they may still allow for many ordinary business transactions with the country at issue, even with respect to the listed entities. The listed entities may not be themselves involved in targeted activity, but they may be identified due to their relationship to government decision-makers (to exert pressure on those decision-makers) or because of their importance to a country's economy or future growth prospects.
- **Special debt and/or equity sanctions.** These relatively complex prohibitions allow for the continuation of day-to-day business with targeted entities while restricting the ability of targets to deal in new or new equity (valuable for, e.g., raising capital for long-term projects). These sanctions have generally been applied to entities within specific economic sectors (e.g., energy) but have also been applied to entities owned or controlled by a target government.
- **Conduct-based sanctions.** These list-based sanctions, as described in an additional resource, are directed not at particular countries or governments but rather at anyone involved in defined types of malicious activity. Persons and entities can be designated for involvement in

terrorism, proliferation of weapons of mass destruction, bribery/corruption, human rights violations, drug trafficking, organized crime, election interference, and cyber-enabled malicious activity. Conduct-based sanctions are meant to identify, disrupt, and deter sanctioned activities.

The key types of sanctions listed above may vary on the above characteristics even within a single category. Nor are these key types of sanctions mutually exclusive (e.g., regime-based sanctions may overlap with special debt and/or equity sanctions).

Sanctions Regimes

Due to the nature of the business of the Company, different regulatory regimes may have jurisdiction over its transactions, Clients, products and services. This section outlines the major sanctions regimes and the basis of their jurisdiction directly impacting the Company's operations.

The United Nations (UN)

Under Chapter VII of the UN Charter, The United Nations Security Council (UNSC) can take action to maintain or restore international peace and security. The UN sanctions are administered by sanctions committees associated with the Security Council and are complemented by Financial Action Task Force (FATF) Recommendations 6 and 7. UNSC resolutions are legally binding to the UN member states.

The Company complies with sanctions restrictions imposed by the UN across all its operations.

The European Union (EU)

Sanctions are one of the EU's tools to promote the objectives of the Common Foreign and Security Policy (CFSP): peace, democracy and the respect for the rule of law, human rights and international law. The EU implements all sanctions imposed by the UN. In addition, the EU may reinforce UN sanctions by applying stricter and additional measures. Where the EU deems it necessary, it may decide to impose autonomous sanctions.

EU restrictive measures only apply within the jurisdiction of the EU, that is: a) within EU territory, including its airspace; b) to EU nationals, whether or not they are in the EU; c) to companies and organisations incorporated under the law of a member state, whether or not they are in the EU. This also includes branches of EU companies in third countries; d) to any business done in whole or in part within the European Union; e) on board of aircrafts or vessels under the jurisdiction of a member state.

The Company complies with sanctions restrictions imposed by the EU across all its operations.

The United Kingdom (UK)

The UK financial sanctions apply, inter alia: a) within the territory and territorial waters of the UK and to all UK persons, wherever they are in the world, b) to all individuals and legal entities who are

within or undertake activities within the UK's territory, c) to all UK nationals and UK legal entities established under UK law, including their non-UK branches; they must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

The Company complies with sanctions restrictions imposed by the United Kingdom to the extent that such sanctions do not contradict the laws of the European Union.

The United States (US)

In terms of applicability, the US sanctions fall into two categories:

- **primary US sanctions:** applicable to US persons, including all US citizens and permanent resident aliens regardless of where they are located, all persons and entities within the US, all US- incorporated entities and their foreign branches. In the cases of certain programs, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S.-origin goods to comply.
- **secondary US sanctions:** when applied, potentially subject non-U.S. persons to sanctions even if they are conducting business entirely outside of the United States and there is no US nexus in a relationship or a transaction. A number of sanctions programmes administered by the Office of Foreign Assets Control (OFAC) of the Department of the Treasury include secondary sanctions, including but not limited to Russia, Iran, Hong Kong/China sanctions programmes.

To the extent that is permissible under the local laws and the EU laws and regulations, the Company complies with both primary and secondary sanctions restrictions imposed by the US. Where compliance with secondary US sanctions is not permissible, e.g., regulation (EC) No 2271/96 and Joint Action 96/668/CFSP of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (OJ L 309, 29.11.1996, pp. 1 and 7), the Compliance Officer must escalate the matter to the Director(s) and the Board of Directors as a whole.

Policy Statement

Under this Sanctions Policy, the Company must:

- Where required by law, block accounts and other assets of sanctioned entities and individuals.
- In all other instances, prohibit or reject unlicensed trade and financial transactions with sanctioned jurisdictions, entities, and individuals.
- Exit relationships with Clients confirmed to be subject to sanctions, regardless of whether this is required by local law in the jurisdiction where the account or relationship is based. In the event that an exit is not permissible under local law, this should be escalated to the Director(s) and the Board of Directors as a whole.
- The Company must not knowingly engage in any transactions and/or business relationships structured to or aimed at the circumvention of applicable sanctions restrictions.

Failure to comply with this Policy may expose the Company to regulatory action or fines, civil or criminal liability as well as possible reputational damage.

Staff responsible for breaches of sanctions related laws and regulations may also be exposed to criminal liability or fines. Staff who fail to comply with this Policy may be subject to disciplinary action, including dismissal.

Roles and Responsibilities

The Board of Directors

The responsibilities of the Board of Directors with regard to the Company's Sanctions Policy shall include:

- Reviewing and approving this Policy as required.
- Ensures effective communication of the importance of sanctions compliance throughout the organisation.
- Provides oversight to ensure the AML/CTF and sanctions compliance function receives adequate support and resources at every organisational level and has sufficient authority and independence to effectively exercise its responsibilities.
- The Board receives and considers regular compliance reports presented by the Compliance Officer, covering both AML/CTF and sanctions compliance.
- Appointing a qualified Compliance Officer with overall responsibility for the proper application the sanctions policy and provides this senior-level officer with sufficient authority that when issues are raised they get the appropriate attention from the Board and the business lines.

The Director(s)

The Director(s) shall receive and evaluate regular compliance reports provided by the Compliance Officer and, where required, authorize changes based on the Compliance Officer's recommendations.

The Director(s) will also receive reports on particularly significant changes that may present risk to the Company as well as conflict of law and make the final decision regarding other sanctions-related issues escalated by the Compliance Officer as required by this Policy.

The Compliance Officer

The responsibilities of the Compliance Officer with regard to the Company's Sanctions Policy shall include:

- undertaking sanctions risk analysis of alerted transactions and/or potential and existing Clients including assessment of documentary evidence provided by Clients;
- proposing any necessary amendments to this Sanctions Policy and submitting them to the Board for approval;
- ensuring that all relevant employees are periodically informed of any changes in sanctions legislation, policies and procedures, as well as current developments and changes in sanctions evasion activities particular to their jobs;
- reviewing Client identification information to ensure that all the necessary information has been obtained.

All Other Employees

All Company employees should maintain continual awareness of the risk that sanctioned parties/transactions pose to the Company and its Client base and must not allow the Company to be used as a conduit for sanctions evasion. To support this, all staff are required to:

- Comply with this Sanctions Policy, related procedures, and applicable sanctions laws and regulations.
- Remain alert and promptly report to the Compliance Officer possible sanctions violations, or Clients found to be engaging in sanctions evasion activities or violations of this Policy or related procedures.
- Refrain from providing advice or other assistance to individuals or entities who seek to violate or attempt to violate any sanctions law or regulation, this Policy, or related procedures.
- Complete all required sanctions compliance training in a timely manner.
- In discussion or correspondence with Clients, staff are strictly prohibited giving any form of advice which might be seen as helping Clients to structure transactions or accounts in a way which could constitute sanctions evasion.

Sanction Screening

The Company must ensure that sanctions screening is performed on existing and prospective Clients, connected parties, transactions and third parties against sanction lists.

The specialized third party risk management solution selected by the Company shall ensure ongoing sanction screening process after a business relationship is established. The potentially matching data from various sanctions and watchlists is compared against the applicant profile to establish an exact match, before a match status is assigned. The following types of status may be assigned:

True positive: Applicant data exactly matches one or several watchlist records.

Potential match: Name of the applicant matches one or several watchlist records, but the age/year of birth data is missing, or the applicant is suspected of committing a crime.

False Positive: Applicant data does not match any of the watchlist records.

- Applicant data matches the watchlist record exactly, but additional information clearly shows that the applicant and the person on the record are different people.
- Applicant data matches the watchlist record, but the record does not include criminal or suspicious information about a person. For example, if the applicant is a crime journalist, and their name features on the article as the author.

Unknown: Applicant name in the document contains only one word.

Applicants with “True Positive” and “Potential Match” statuses are delegated to the Compliance Officer for further processing. If applicants are declined based on a watchlist match, they are assigned a respective rejection tag:

- Sanctions
- PEP
- Criminal records
- Adverse Media

The sanction lists screened include (non-exhaustive list of sources):

European External Action Service (EEAS)	
CFSP Consolidated Financial Sanctions List	Consolidated list of all persons, groups, and entities subject to EU financial sanctions. The CFSP list is the official EU database. It includes the financial sanctions from the anti-terror regulations, the country-specific embargo regulations, and other sanctioning regulations such as those against cybercrime or serious human rights violations.
Council of the European Union	
EU – Russia embargo: Restrictions for	This list contains Russian organizations concerned by the sanctions laid down in light of Russia’s actions to undermine Ukraine's stability. The list contains the entries of annex IV of Council Regulation (EU) No. 833/2014

dual-use goods intended for listed organisations.	of July 31, 2014, and amended by Council Regulation (EU) No. 960/2014 on September 8, 2014.
EU – Russia embargo: Restrictions on access to the capital market.	It lists Russian entities that are more than 50% state-owned and are subject to the sanctions laid down with respect to Russia's actions contributing to Ukraine's destabilization. The list consolidates the entries of annex III of Council Regulation (EU) No. 833/2014 of July 31, 2014, and of annexes II and III of the related amending regulation 960/2014 of September 8, 2014.
UK lists - HM Treasury – The UK government's economic and finance ministry	
BOE Consolidated List of Financial Sanctions Targets in the UK	Database of all listed persons, groups, and entities subject to financial sanctions by the UN and the UK.
List of entities subject to capital market restrictions (former Ukraine Sovereignty List)	The List of entities subject to capital market restrictions, provided by HM Treasury, lists Russian entities that are more than 50 % state-owned and are subject to the sanctions laid down with respect to Russia's actions contributing to Ukraine's destabilization. These sanctioned organizations are subject to other financial and investment restrictions and are therefore not included in the OFSI Consolidated List of Financial Sanctions Targets in the UK (BOE list). The list consolidates the entries in Schedule 2 of the Russia (Sanctions – EU Exit) Regulations 2019.
Foreign, Commonwealth & Development Office Sanctions List	With the UK Sanctions List, the British government provides a list of persons, entities, or means of transport that are subject to both financial sanctions and restrictions on entry, trade, and other restrictions depending on the respective national sanctions regimes of the United Kingdom. This is based on the Sanctions and Anti-Money Laundering Act 2018 (SAML A) and UN Security Council resolutions.
US lists - Department of Commerce – Bureau of Industry and Security (BIS)	
Denied Persons List	The Denied Persons List contains the names of those who have violated US export regulations and against whom the Bureau of Industry and Security has therefore issued a denial order. The listed persons have been denied all exporting privileges, meaning that no US goods can be provided to or purchased from them. Businesses that violate such a denial order are in violation of US export regulations and risk being listed on the DPL themselves.

Entity List	The Entity List lists persons and entities implicated by American authorities as posing a significant threat in the proliferation of weapons of mass destruction or missile technology.
Military End User List	The Military End User List contains companies that are classified by the US government as military end users. According to the findings of the US authorities, the listed companies pose a significant risk of a military end-use of the goods from Supplement No. 2 to Part 744 EAR.
US lists - Department of the Treasury – Office of Foreign Assets Controls (OFAC)	
Specially Designated Nationals List	The SDN list contains the names of all persons, groups, and entities worldwide implicated by American authorities as involved in terrorist activities threatening US security. Active SDN sanctions programs: - Balkans-Related Sanctions - Belarus Sanctions - Blocking Property of Certain Persons Associated with the International Criminal Court Sanctions - Burundi Sanctions - Central African Republic Sanctions - Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA) - Counter Narcotics Trafficking Sanctions - Counter Terrorism Sanctions - Cuba Sanctions - Cyber-related Sanctions - Democratic Republic of the Congo-Related Sanctions - Foreign Interference in a United States Election Sanctions - Global Magnitsky Sanctions - Hong Kong-Related Sanctions - Iran Sanctions - Iraq-Related Sanctions - Lebanon-Related Sanctions - Libya Sanctions - Magnitsky Sanctions - Mali-Related Sanctions - Nicaragua-Related Sanctions - Non-Proliferation Sanctions

	- North Korea Sanctions - Rough Diamond Trade - Somalia Sanctions - Sudan and Dafur Sanctions - South Sudan-Related Sanctions - Syria Sanctions - Syria-Related Sanctions - Transnational Criminal Organizations - Ukraine-/Russia-Related Sanctions - Venezuela-Related Sanctions - Yemen-Related Sanctions - Zimbabwe Sanctions
OFAC-CSL Consolidated Sanctions List (OFAC)	With the Consolidated Sanctions List, the OFAC provides a consolidated list of all persons and entities of its non-SDN sanctions programs. The Consolidated Sanctions List is not part of the Specially Designated Nationals and Blocked Persons List (SDN) of the OFAC. Nevertheless, it is possible that individual entries are also included in the SDN list. The OFAC Consolidated Sanctions List includes the following sanctions lists, for example: - Foreign Sanctions Evaders (FSE) List - Sectoral Sanctions Identification (SSI) List - Palestinian Legislative Council (NS-PLC) List - Non-SDN Iranian Sanctions Act (NS-ISA) List - List of Foreign Financial Institutions Subject to Correspondent Account or Payable- Through Account Sanctions (CAPTA List) - Non-SDN Menu-Based Sanctions (NS-MBS) List - Non-SDN Communist Chinese Military Companies (NS-CCMS) List
United Nations Security Council	
UN Consolidated United Nations Security Council Sanctions List	Consolidated list of all persons, groups, and entities subject to UN Security Council sanctions. The consolidation is to facilitate the implementation of the measures introduced by the UN. The listed persons and entities are subject to various sanctions regimes that provide for different measures.

In case of positive matches against sanctions lists, the action performed by the Compliance Officer will be in line with the requirements of a specific sanctions program (e.g. asset freeze, rejection, or debt/equity restrictions etc.) as well in consideration with any potential conflict of law.

Sanctions Evasion

UN, U.S., and EU sanctions programs include prohibitions on evasion of their principal provisions, with authorities increasingly focusing on evasion as its own category of sanctioned activity.

Examples of attempts to evade sanctions may include:

- Client (natural or legal person) who is not on any applicable sanctions list purchases cryptocurrency on behalf of a business entity owned by a sanctioned party.
- Where a payment is rejected by the Company, and the Client re-issues the payment after changing or removing information, thereby making it difficult to identify and restrict payments to and from sanctioned parties or countries (activity known as “wire stripping”).
- Client physically located in the U.S. utilizes VPN to mask IP address, thereby making it possible to engage in a transaction that is permitted in the EU but prohibited for the US Persons; or
- Payments to a party who is located in a non-sanctioned jurisdiction and acting as a “front company” or acting as an intermediary for sanctioned parties or parties in sanctioned jurisdictions.

Potential sanctions evasion activities may be detected by the Company’s staff at various levels of seniority and across different functions, i.e. through engagement with the existing or prospective Clients, business partners, transaction monitoring, ongoing due diligence (ODD) and other. All suspected attempts to evade or circumvent sanctions must be immediately escalated to the Compliance Officer who, after assessing the scenario, may decide that the case should be escalated to the relevant authorities.

In addition to sanctions screening, the Company utilizes its AML/CTF transaction monitoring, Client due diligence (CDD) and other processes to identify potential sanctions evasion activities by its Clients, third parties, and staff.

When performing the review and approval of Clients identified as high-risk according to the Company’s ML/TF risk assessment methodology, the Compliance Officer also reviews the Client for potential sanctions evasion activities.

The results of the investigation shall be recorded in line with the Company’s AML Policy. Potential sanctions evasion activities, if detected, must be included in the AML/CTF and sanctions compliance reporting documents submitted by the Compliance Officer to the Executive Director(s) and the Board.

Asset Freezing

For the purpose of this Policy, freezing, also known as “blocking”, refers to a form of controlling assets in which a sanctioned party has an interest. While title to blocked property remains with the

sanctioned party, the exercise of the powers and privileges normally associated with ownership is prohibited without authorisation from the sanctioning competent authority. Blocking immediately imposes an across-the-board prohibition against transfers or transactions of any kind with regard to the property.

“Assets” refer to tangible or intangible resources with economic value that an individual, corporation or country owns or controls with the expectation that it will provide future benefit. In case of the Luckyroo N.V, the assets include cryptocurrency and fiat currency.

Sanctions Compliance Training

Sanctions compliance training is one of the pillars of the Company’s sanctions compliance programme. The Compliance Officer is responsible for reviewing and updating (where required) the sanctions compliance programme.

The compliance training falls under two categories:

1. Annual General Audience (All Staff) training,
2. Risk-Based/Ad-Hoc training to Staff who perform functions considered to be higher risk from a sanctions perspective, such as roles that entail Client contact, processing Client transactions, or otherwise evaluating Client data, must receive additional targeted training to supplement the annual sanctions learning provided to all Staff.

All Staff must receive annual General Audience (All Staff) sanctions compliance training. All new hires must receive the training within 30 (thirty) days of on-boarding. The General Audience (All Staff) sanctions compliance training shall include, at a minimum:

- Major sanctions regimes (UN, EU, UK, US).
- Major sanctions programs and requirements.
- Sanctions evasion methods and techniques.
- Sanctions risk indicators (‘red flags’).
- Sanctions compliance roles and responsibilities of the Company’s staff.
- Consequences of non-compliance.

All training records, including the training content (e.g. presentation slides, post-course assessment) and attendance records must be kept in line with the record-keeping requirements.

Outsourcing

Where a sanctions compliance activity is outsourced to an entity outside the Company, the Company is ultimately accountable for ensuring that such activities are undertaken in compliance with the requirements of this Policy, and all applicable sanctions laws, rules and regulations.

Record-Keeping And Record Retention

The Company adopts one set of record-keeping and record retention rules and requirements to all sanctions-related items as set by the Company's AML Policy.

Appendix IV

Client Acceptance Policy

Statement of the Policy

Luckyroo N.V. has implemented this Customer Acceptance Policy ("CAP") to establish clear standards and procedures for assessing and approving customers who wish to access its online gaming and betting services. The purpose of this policy is to protect the company from being exploited for unlawful activities such as money laundering, terrorist or proliferation financing, sanctions evasion, fraud, and other illicit behaviour, while ensuring full compliance with Curaçao's legal and regulatory framework.

This policy is aligned with the guidance of the Curaçao Gaming Control Board and forms part of Luckyroo N.V.'s wider Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) program. It also incorporates international best practices, including the Financial Action Task Force (FATF) Recommendations, the European Union Anti-Money Laundering Directives, and the Wolfsberg Principles.

To comply with Curaçao legislation, the policy integrates the requirements of the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

This policy applies to all directors, officers, employees, contractors, and any third parties involved in onboarding and verification activities. No customer is allowed to deposit, withdraw, or engage in gaming activities until they have met all acceptance criteria and successfully completed the required identification, verification, and screening procedures.

2. Scope of the Policy

This policy applies to every individual or entity that wishes to open an account with Luckyroo N.V., regardless of the registration channel used. This includes account creation through the company's official website, mobile applications, affiliate partnerships, or third-party platforms.

The provisions of this policy cover the entire customer relationship, starting from the initial registration and continuing through all stages of account activity until closure or termination. It applies to all products and services provided by Luckyroo N.V. under its Curaçao gaming licence OGL/2024/1371/0694.

3. Customer Acceptance Integration

Luckyroo N.V. only accepts customers who meet all applicable legal, regulatory, and internal compliance requirements. Every applicant must be verified to confirm they have reached the legal age for gambling, which is at least eighteen (18) years or higher where required by the laws of their jurisdiction. Applicants are also required to provide accurate and verifiable personal details,

including their full legal name, date and place of birth, nationality, and current residential address.

The company does not allow the registration of customers who are residents of, located in, or conducting transactions from jurisdictions restricted under Curaçao's regulatory framework, international sanctions regimes, or Luckyroo N.V.'s internal prohibited jurisdictions list. As part of the onboarding process, every applicant is screened against international and local sanctions lists, including those maintained by the United Nations, the European Union, the U.S. Office of Foreign Assets Control (OFAC), the U.K. Office of Financial Sanctions Implementation (OFSI), the Sanctions National Ordinance, the Kingdom Sanction Act, and any lists issued by the Curaçao Gaming Control Board.

All funds used for gaming and betting activities must come from legitimate, lawful sources. Where the company's risk assessment indicates the need for additional scrutiny, customers are required to provide supporting documentation to verify the origin of their funds and, if applicable, their source of wealth. Luckyroo N.V. also reserves the right to deny service to any individual or entity with a history of fraudulent behaviour, chargebacks, bonus abuse, self-exclusion due to problem gambling, or any other violation of gambling regulations.

4. Risk-Based Approach

Luckyroo N.V. applies a thorough Risk-Based Approach (RBA) during both the onboarding process and the ongoing assessment of its customers. This approach ensures that the level of due diligence applied is proportionate to the customer's individual risk profile. The evaluation takes into account a range of factors, including the customer's personal and financial background, the types of products and services they use, any geographic risks associated with their location or funding sources, and potential risks arising from the technologies or channels they use to access the platform.

Customer Risk Profile

Luckyroo N.V. assesses every prospective customer to determine their level of exposure to risks such as money laundering, terrorist financing, or proliferation financing. This assessment ensures that due diligence measures are applied proportionately to each customer's profile.

Customers who present clear, transparent, and verifiable financial backgrounds — for example, those with stable employment in low-risk sectors and gambling activity that aligns with their declared income — are typically classified as low risk.

Conversely, customers may be considered high risk if they exhibit certain characteristics, such as having multiple or opaque income sources, employment in industries with elevated AML risk like cryptocurrency or unregulated financial services, or transaction patterns that appear inconsistent with their stated financial profile. Politically Exposed Persons (PEPs), their family members, and close associates are automatically categorised as high risk and are subject to stricter controls.

High-risk cases are managed through Enhanced Due Diligence (EDD), which may include more detailed verification procedures, additional documentation requirements, and ongoing monitoring. Examples of high-risk scenarios include:

- Customers with multiple or irregular income sources, who must provide evidence such as payslips, tax returns, business records, or investment statements.
- PEPs or their close associates, whose accounts require senior management approval, detailed source-of-wealth and source-of-funds checks, and ongoing enhanced monitoring.

- High or disproportionate spenders, where gambling activity exceeds what would reasonably match a customer's financial profile, requiring additional documentation and scrutiny.
- Customers exhibiting sudden, unexplained changes in gambling patterns or those using third parties to transact on their behalf, triggering immediate review and investigation.
- Attempts to operate multiple accounts, which are identified through internal monitoring systems and consolidated for a full transactional review.
- Unknown customers attempting to redeem large volumes of chips, or customers linked to junket operators, both of which require strict verification and EDD measures.

Luckyroo N.V. also conducts ongoing monitoring to ensure customer risk profiles remain accurate and up to date. Periodic reviews are scheduled, and additional checks are triggered whenever significant changes are detected, such as unusual transaction patterns, large unexplained deposits, or changes to a customer's personal or financial circumstances. Where risk levels increase, the company applies enhanced controls — including EDD, closer transaction monitoring, or restrictions on account activity — to ensure risks remain effectively mitigated and regulatory obligations are consistently met.

Geographic Risk Assessment

Luckyroo N.V. uses a dynamic geographic risk framework to evaluate potential risks linked to a customer's location or the origin of their funds. This framework is regularly updated based on trusted and authoritative sources, including publications and lists from the Financial Action Task Force (FATF), the Caribbean Financial Action Task Force (CFATF), the European Commission's high-risk country listings, the U.S. Office of Foreign Assets Control (OFAC), the U.S. Department of State's International Narcotics Control Strategy Reports, and Transparency International's Corruption Perceptions Index.

Customers from jurisdictions subject to international sanctions are not accepted under any circumstances. Those from high-risk jurisdictions may be considered for onboarding only after Enhanced Due Diligence (EDD) is completed and senior compliance approval is granted.

Jurisdictions are considered high risk when they exhibit one or more of the following characteristics: inadequate anti-money laundering and counter-terrorist financing frameworks or poor enforcement of such measures, systemic corruption that increases the likelihood of illicit funds entering the platform, association with international sanctions related to terrorism or weapons proliferation, or active presence of terrorist organizations.

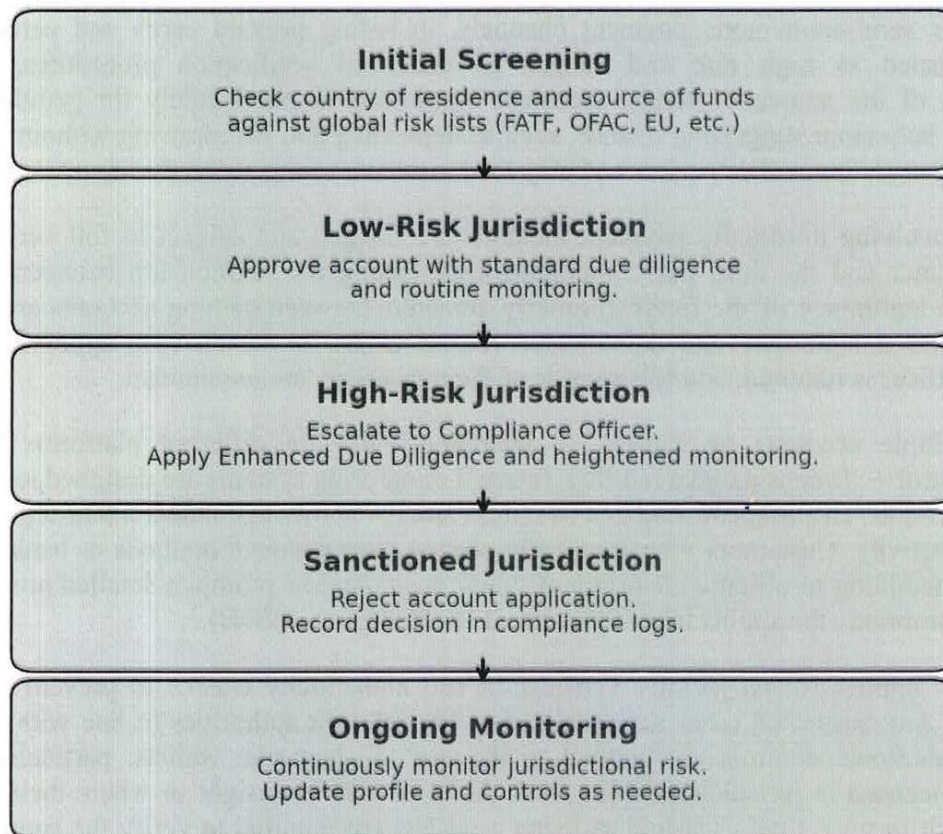
To maintain accurate classifications, Luckyroo N.V. continuously monitors relevant global and regional sources. These include FATF high-risk and monitored jurisdictions lists, CFATF advisories, the European Commission's list of countries with strategic AML/CFT deficiencies, OFAC sanctions lists, U.S. State Department reports, and corruption indices or reports indicating potential links to terrorist financing.

When a customer's country of residence or source of funds appears on a high-risk or sanctioned list, the case is escalated to the Compliance Officer. In such instances, EDD measures are mandatory, including in-depth identity verification, a thorough review of the source of funds and source of wealth, and enhanced transaction monitoring for as long as the relationship continues.

Geographic Risk Assessment Process

1. **Initial Screening** – The customer’s location and funding sources are checked against global lists and reports to determine their risk level.
2. **Low-Risk Jurisdiction** – The account may be approved under standard due diligence procedures with routine monitoring.
3. **High-Risk Jurisdiction** – The application is escalated to compliance for review. Onboarding is only approved if all EDD criteria are satisfied, and heightened monitoring is applied.
4. **Sanctioned Jurisdiction** – The application is rejected, and records are retained in compliance logs.
5. **Ongoing Monitoring** – Customer profiles are dynamically updated, and additional controls are applied if jurisdictional risk changes over time.

Geographic Risk Assessment Flow



Product, Service, and Transaction Risks

The level of risk associated with a customer is also determined by the products, services, and transaction types they use. Certain activities naturally carry a higher degree of risk due to reduced transparency and traceability. Examples include peer-to-peer transfers, the purchase or exchange of gaming tokens, or the use of anonymous or semi-anonymous payment methods such as prepaid cards or specific cryptocurrencies.

Accounts that are used mainly for financial transactions rather than genuine gameplay — such as those making large deposits followed by minimal or no betting activity before withdrawals — are treated with caution and subject to closer review. Likewise, the use of payment instruments not registered in the account holder's name automatically triggers additional verification measures to confirm legitimacy.

To mitigate these risks, Luckyroo N.V. actively monitors and manages several key risk areas. Funds deposited into gaming accounts must always originate from lawful and verifiable sources. If there are signs that funds may be linked to criminal activities such as fraud, theft, or trafficking, customers are required to provide evidence of the legitimate source of those funds, and any suspicious transaction is reported to the Financial Intelligence Unit (FIU) in line with legal requirements.

Anonymous or semi-anonymous payment channels, including prepaid cards and certain virtual assets, are treated as high risk and subject to enhanced verification procedures, with full documentation of the source of funds. Accounts must also be used solely for genuine gaming purposes. Any behaviour suggesting misuse, such as depositing and withdrawing without significant gameplay, triggers an immediate review and may lead to account suspension during investigation.

Transactions involving third-party payment methods are flagged and subject to full verification of both the customer and the third party, including establishing the relationship between them and confirming the legitimacy of the funds. Similarly, transfers between gaming accounts are generally prohibited unless a legitimate and documented reason exists, in which case approval from the Compliance Officer is required, and full records of the transaction are maintained.

Operating multiple accounts or wallets — including those on different platforms under the company's control — is considered a red flag. Internal monitoring systems are designed to detect and link related accounts, ensuring consolidated oversight and the ability to conduct a thorough review of all connected activity. Customers who frequently change their payment methods or banking details may also be attempting to obscure the origin of funds; such patterns prompt a detailed profile review and, where appropriate, the application of Enhanced Due Diligence (EDD).

Luckyroo N.V. applies robust identity verification and authenticity checks to prevent and detect identity fraud. Any suspected cases are escalated to the relevant authorities in line with regulatory obligations. Additional controls are applied to the use of electronic wallets, particularly where providers are licensed in jurisdictions with weak AML or CTF oversight or where their structures make it difficult to trace funds. Customers using e-wallets are required to verify the source of their funds, and the provider's licensing and compliance standards are checked before any transaction is approved.

Channel and Technology Risk

The level of risk associated with a customer also depends on the channels and technologies used to access Luckyroo N.V.'s services. Remote onboarding, while convenient, carries a higher risk of identity fraud or impersonation. To address this, the company relies on advanced digital Know Your Customer (KYC) solutions that include biometric verification, document authenticity checks, geolocation validation, and multi-factor authentication.

Before introducing any new technologies, payment solutions, or platform features, Luckyroo N.V. conducts a comprehensive risk assessment to ensure the innovation cannot be misused for money laundering, fraud, or other illicit purposes.

Several factors are monitored closely to manage channel and technology-related risks. Any method that allows customers to remain anonymous is considered high risk and triggers enhanced verification measures. These measures include identity document validation, biometric checks, and real-time screening against sanctions and Politically Exposed Person (PEP) lists.

Remote interactions, although common in the industry and not inherently high risk, still demand strong safeguards. Luckyroo N.V. uses secure verification technologies such as biometric checks, liveness detection, and automated document validation to prevent impersonation and fraud during onboarding and transactions.

When third parties are involved in customer interactions, the risk profile increases, especially if the intermediary is not subject to AML/CFT obligations. In such cases, Luckyroo N.V. performs due diligence not only on the customer but also on the third party. This process includes verifying the intermediary's regulatory status, assessing its compliance framework, and ensuring all provided information is accurate and verifiable.

Channel and Technology Risk - Staff Checklist

Anonymous Channels Apply enhanced verification: ID validation, biometric checks, and sanctions screening.
Remote Onboarding Use biometric authentication, liveness detection, and document authenticity checks.
Remote Transactions Enable multi-factor authentication and monitor for device/IP anomalies.
Third-Party Interactions Verify intermediary licensing, assess AML/CTF framework, and validate provided data.
New Technologies Perform pre-launch risk assessment and compliance approval.

Risk Indicators

Luckyroo N.V. applies a structured set of risk indicators to assess the level of risk associated with every customer relationship. These indicators form part of the company's Risk-Based Approach (RBA) and ensure that the level of due diligence applied is always proportionate to the customer's overall risk profile.

The evaluation covers multiple categories:

- **Customer Risk Profile** – factors such as multiple or irregular income sources, Politically Exposed Persons (PEPs), high or disproportionate spending, sudden changes in spending behaviour, involvement of third parties, multiple accounts, unknown chip redemptions, or links to junket operations.
- **Product, Service, and Transaction Risk** – warning signs such as proceeds of crime, anonymous or unregulated payment methods, misuse of accounts, third-party funding, frequent changes in payment instruments, identity fraud, or the use of multiple e-wallets.

- **Geographic Risk** – customers connected to jurisdictions with weak AML/CFT frameworks, high levels of corruption, international sanctions, terrorism links, or countries listed by FATF, CFATF, OFAC, or Transparency International's CPI.
- **Channel and Technology Risk** – customers accessing services through anonymous or unverified channels, onboarding remotely without sufficient identity validation, or relying on unregulated third-party intermediaries.

To determine the customer's overall risk, the company uses an internal Risk Calculator that assigns a weighted score to each indicator. The total score determines the customer's classification:

Risk Level

Requirements

Low Risk Standard Customer Due Diligence (CDD) applies, with documentation limited to what is legally required or triggered by a change in risk profile.

Medium Risk Standard CDD plus additional verification steps and closer ongoing monitoring.

High Risk Full Enhanced Due Diligence (EDD), senior management approval prior to onboarding, and enhanced ongoing monitoring.

This risk-scoring approach ensures a consistent and methodical assessment of customers, allowing the company to allocate its resources effectively and meet its regulatory obligations.

Risk Indicators Table

Factor	Low Risk	Medium Risk	High Risk
Purpose of Account	Recreational or casual gaming.	Professional-level gambling or consistent high-stakes play.	Bonus exploitation or behaviour aimed at financial abuse of promotions.

Source of Funds	Regular salary, savings, pensions, or other low-risk income.	Business income, legitimate casino winnings, sale of personal assets, inheritance, or documented loans/gifts from family or friends.	Unverified cryptocurrency, offshore accounts, or other unverifiable sources.
Source of Wealth	Long-term employment income, ownership of established businesses, verified inheritance, or steady investment growth.	Sale of property or business, significant lottery or gambling winnings.	High-risk investments such as cryptocurrency or forex trading, offshore holdings, or unverifiable assets.
Transaction Frequency	Occasional, typically monthly.	Regular, often weekly.	Frequent, typically daily.
Transaction Value (NAF)	Up to 1,000.	Between 1,000 and 4,000.	Over 4,000.
Incoming Payments	Standard bank transfers or debit/credit card deposits.	E-wallet or prepaid card deposits.	Cryptocurrency, third-party funding, deposits from high-risk jurisdictions, unusually high deposits, or use of unregulated processors.
Outgoing Payments	Normal withdrawals of winnings or deposit refunds.	Bonus-related cash-outs, frequent withdrawals, or large single withdrawals above 4,000.	Cryptocurrency withdrawals, third-party payments, chargebacks, or suspicious withdrawal patterns linked to other accounts.

Gaming Behaviour	Casual, moderate, and consistent play patterns.	Frequent high-stakes betting, extended play sessions, or fluctuating wagering amounts.	Aggressive betting patterns, rapid stake increases, loss-chasing, multiple accounts, collusion, or other fraudulent indicators.
Payment Channels	Traditional bank transfers.	Verified e-wallets.	Cryptocurrency or other anonymous or unverified payment methods.
Adverse Media	No negative information identified.	Questionable or unverified reports of misconduct.	Confirmed involvement in criminal or illicit activities.

Guidance on Using the Risk Indicators

These indicators are designed to help staff assign an accurate risk profile to each customer during onboarding and throughout the customer relationship. Each factor should be assessed individually, and the combined results should inform the overall risk classification.

- Customers with mostly low-risk indicators are assigned a low-risk profile and subject to standard Customer Due Diligence (CDD).
- Customers with a mix of low and medium-risk indicators are classified as medium risk and require additional verification and closer monitoring.
- Customers displaying one or more high-risk indicators must undergo Enhanced Due Diligence (EDD), senior management approval before onboarding, and ongoing heightened monitoring.

Risk profiles should be reviewed regularly and adjusted when customer behaviour, transaction patterns, or external risk factors change. This approach ensures that the company's risk management remains dynamic and aligned with regulatory expectations.

5. Onboarding Procedures

Luckyroo N.V. follows a structured and well-documented onboarding process to ensure that only customers meeting the company's acceptance standards gain access to the platform. No account is activated until the customer has successfully completed all required identification, verification, and sanctions screening steps.

During registration, customers are required to provide their full legal name, date and place of birth, nationality, residential address, and an official identification number such as a passport or national

ID.

Every applicant is screened against international sanctions and Politically Exposed Person (PEP) databases using automated tools to ensure comprehensive coverage. Any potential matches or alerts are reviewed manually by trained compliance officers to confirm accuracy and rule out false positives.

If a customer is identified as high risk during the initial assessment, additional verification is required. This includes providing documentation to confirm the legitimacy of their funds and, where relevant, the source of their wealth. Acceptable documents may include recent bank statements showing income deposits, business account records or financial statements, tax returns, contracts of property or asset sales, and investment account statements. These enhanced measures ensure that the company meets regulatory expectations and maintains a strong control framework to protect the platform from misuse.

Client Identification requirements and verification procedures

This section refers to individuals who directly or indirectly establish a business relationship with the Company (e.g. direct Clients, beneficial owners, authorized persons, etc.). The Company should be satisfied that it is dealing with a real person and obtain sufficient evidence of identity to establish that a prospective Client is who he/she claims to be.

Document verification is intended to prevent the following issues:

Forgery
Data tampering
Photo replacement
Fraud
Using document printouts
Other manipulation

The ID document must contain as minimum the following information:

Owner full name
Owner full date of birth
Document number
Validity data (issue date or validity period)
Owner photo
Owner signature (if applicable)

The ID document should meet the following requirements:

- The document is valid for at least one month from the upload date.
- The document is not scratched, stained, or torn.
- The applicant full name, date of birth and other important information is present and can be read.

Uploading the photo of an ID document

The photo of the ID document uploaded to the system should meet the following requirements:

The uploaded file is an original photo (static image) or scan (not a screenshot or a photo uploaded from social networks) in JPG, JPEG, PNG, PDF.

If the document has data on the front and back, both sides should be uploaded.

The size of the uploaded file is no less than 100 KB or 300 DPI.

The photo is in color.

The information in the document is readable.

All corners of the document are visible and no foreign objects or graphic elements are present.

The uploaded photo has not been edited with any software or converted to PDF.

The document is not digital (in most cases).

Checking the image for authenticity

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or software-specific tags, sections, and so on. An extensive database of camera and software signatures are utilized to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Document data validation

At the final step, the data extracted from the document is checked against various sources, including sanctions and watchlist databases.

1. Proof of address verification

a. Face-to-face procedures

For the purpose of face-face Client identification, the Compliance Officer shall inspect the person's original Proof of Address (PoA) documentation and make a certified true copy to be maintained as evidence of verification.

b. Non-face to face procedures

The process of Proof of Address (PoA) document verification for non-face to face Clients consists of the following steps:

- **Uploading a PoA photo.**

By default, the system accepts PoA documents that have been issued within the last 3 months.

- **Checking the image for authenticity.**

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or software-specific tags, sections, and so on. An extensive database of camera and software signatures are utilized to

determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Each image receives a digital trust score:

- Low – red (high risk of editing).
- Acceptable – yellow (there might be something to take a closer look at).
- Normal – green (a trusted and authentic image).

- **Checking the integrity of the image.**

Integrity checks are designed to ensure the uploaded image represents an official document by comparing it with a template from a database of original documents. Integrity checks consist of:

- General conformity to the template.
- Font originality and compliance with the relevant standards (width, spaces between the letters, and so on).
- Required fields and inscriptions.

- **Data extraction** (full name, home address, issue date).
- **Data validation** (whether the address is complete, if it exists and if it is really a home address).

To ensure the completeness and consistency of the extracted address data, external map services, such as Google Maps, Open Street Map, and others, are utilized allowing the Compliance Officer to see the applicant's geolocation in the Dashboard.

Supported PoA Documents

Common proof of residency examples:

- Tax bill (not older than 3 months).
- Mortgage statement.
- Certificate of voter registration.
- Correspondence with a government authority regarding the receipt of benefits such as a pension, unemployment benefits, housing benefits, and so on.
- Cable internet/TV bill (but not from satellite TV companies or for other wireless telecommunication services).
- Landline telephone bill.
- Bank statement with the date of issue and the name of the person (the document must be not older than 3 months).
- Utility bill for gas, electricity, water, internet, etc. linked to the property (the document must not be older than 3 months).
- A lease agreement that is current and has the signatures of the landlord and the tenant.
- Rent bills issued by a real estate rental agency.
- Credit card statement issued by a bank.

- Letter from a recognized public authority or public servant (any government-issued correspondence not older than 3 months).
- Employer's certificate for PoA.
- House purchase deed.
- The document must contain the full name, home address, and the document issue date (in most cases). Both paper documents and electronic documents (in PDF) are accepted.

Alternative proof of residency examples

The following documents can also be accepted as valid PoA, but only if they contain an address:

- Passport
- Identity card
- Driving license
- Residence permit (EU samples containing address)

**** The same document cannot be used to confirm both an identity and a place of residence. So, if an applicant submits an ID document as PoA, they should use another document to confirm their identity.*

Documents which are not acceptable as Proof of Address, include:

- Old government-issued correspondence (older than 3 months)
- Old bank statements (older than 3 months)
- Old utility bills linked to the property (older than 3 months)
- Pension statements
- Bank references
- Insurance policies
- Mobile phone bills
- Medical bills
- Receipts for purchases
- Insurance statements
- Documents stating PO Box addresses
- Checks
- Envelopes and parcels showing your name and an address
- Prepaid card invoices
- Mobile sim cards+ bills issued to a business address
- Bills from debt collection agencies
- Bills from fintech companies
- Papers referring to discount cards which cannot be considered as bank cards
- Car rent bills

Source of Funds (SoF) and Source of Wealth (SoW)

SoF refers to origin of funds being deposited, received, or transferred with the Company. SoF tells us where the money is coming from, which can be proven through bank statements, tax returns or the Company financials, etc.

Typically, SoW is requested when establishing business relationships or performing EDD, SoF is requested when there is a need to understand what the origin of a transaction is.

Examples of SoW and SoF and supporting documentation that can be provided, include:

Income category	Documents required
Income from salary	• Pay slips for the past 3 months and bank statement showing the salary being paid into this bank account; • Audited personal tax statement.
Inheritance	• Grant of Probate (with a copy of the Will) clearly showing the amount of inheritance and a bank statement showing these funds being deposited into the account; • Signed letter from a licensed solicitor or estate trustees on letter-headed paper clearly indicating the amount of inheritance, accompanied by updated proof of the solicitor's regulated status and a bank statement showing these funds being deposited into the account.
Gift/donation	• Notarized gift/ donation letter and a bank statement showing these funds being deposited into the account; • Gift agreement and a bank statement showing these funds being deposited into the account.
Savings/deposits	• Savings statement; • Bank statement.
Government grants (retirement income, grants for veterans, research grant, etc.)	• Type of received grant and a bank statement showing these funds being deposited into the account; • Documents confirming/ proving received grant and a bank statement showing these funds being deposited into the account.
Company profit / dividends	• Dividend contract note or equivalent and a bank statement showing these funds being deposited into the account; • Copy of latest audited financial statements; • Tax declaration form.
Loan or investment	• Loan/Investment agreement or other documents confirming the agreement and a bank statement showing these funds being deposited into the account.

Sales (of property, goods, shares, etc.)	● Copy of contract of buy/sale/production and a bank statement showing these funds being deposited into the account; ● Prove of e-shop sale report (screenshot) with the list of items sold and a bank statement showing these funds being deposited into the account; ● Shipping documents and a bank statement showing these funds being deposited into the account; ● Proof of delivery and a bank statement showing these funds being deposited into the account; ● Customs declaration; ● Audited financial report; ● Tax report; ● Statement evidencing the money and a bank statement showing these funds being deposited into the account.
--	---

6. Ongoing Monitoring

Luckyroo N.V. recognises that customer acceptance is an ongoing process rather than a one-time activity. Continuous monitoring is essential to ensure that customer behaviour remains consistent with the profile established during onboarding and that any irregularities or deviations are promptly identified and addressed.

The company uses automated transaction monitoring systems to detect patterns of unusual or suspicious behaviour. Alerts are generated for activities such as deposits or withdrawals that do not match the customer's declared profile, rapid movement of funds without meaningful gameplay, the use of multiple or unusual payment methods, or patterns that may suggest collusion, chip-dumping, or other prohibited activities.

Each alert is reviewed by trained compliance officers, who assess the circumstances and determine whether further investigation or escalation is needed.

In addition to real-time monitoring, the company conducts periodic reviews of customer profiles on a risk-based schedule to ensure risk ratings remain accurate. If there are material changes in a customer's situation, such as relocation to a high-risk jurisdiction, significant increases in transaction values, or changes in funding methods, the customer's risk profile is immediately reassessed. Where necessary, enhanced monitoring and other controls are applied to maintain compliance and mitigate potential risks.

7. Prohibited clients and transactions

Certain types of Client/transactions are not accepted for establishing business relationships or conducting transactions in order to reduce the risk that the services and products of the Company may be used for money laundering or terrorist financing or other illicit purposes and at the same time for protect the Company from the financial, reputational and legal risks.

Consequently, it is strictly prohibited to:

- c. Establish a business relationship with Clients who fail or refuse to submit the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification.
- d. Establish a business relationship and/or conduct transactions with natural or legal persons against which sanctions prohibiting such relationship/transactions are imposed in accordance to the Company's Sanctions Policy (Appendix II).
- e. Conclude or implement any business relationship with a credit institution or other financial institution or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions or legal person that is incorporated in a jurisdiction in which it has no physical presence, involving meaningful management and which is unaffiliated with a regulated financial group (i.e. shell company) or is known to permit accounts to be held by a shell bank.
- f. Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons whose activities are related to criminal activity including (but not exhaustive)
 - Terrorist offences, offences related to a terrorist group and offences related to terrorist activities as set out on Titles II and III of Directive (EU) 2017/541 (replacing Framework Decision 2002/475/JHA on combating terrorism)
 - Any of the offences referred in article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;
 - The activities of criminal organizations as defined in Article 1(1) of Council Framework Decision 2008/841/JHA on the fight against organized crime;
 - Trafficking in human beings and migrant smuggling, including any offence set out in Directive 2011/36/EU;
 - Sexual exploitation, including any offence set out in Directive 2011/93/EU;
 - Fraud affecting the Union's financial interests, where it is at least serious, as defined in Article 1 (1) and Article 291) of the Convention on the protection of the European Community's financial interests;
 - Corruption, including any offence set out in the Convention on the fight against corruption involving officials of the EU Communities or officials of Member States of the EU;
 - All offences, including tax crimes relating to direct taxes and indirect taxes and as defined in the national Laws of Lithuania and which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, if there is a legal threshold by Law for such offences, all offences punishable as above for a minimum of more than six months;
 - Counterfeiting of currency, including any offence set out in Directive 2008/99/EC;
 - Cybercrime, including any offence set out in the Directive 2013/40/EU;

- g. Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons where:
- Legal entities are owned through bearer instruments;
 - Legal entities are involved in the adult industry;
 - Legal entities are involved drugs industry;
 - Legal entities are involved in arms industry;
 - Specially Designated Nationals and Blocked Persons (SDNs);
 - Clients acting on behalf of Specially Designated Nationals and Blocked Persons (SDNs);
 - Clients whose source of funds (SoF) and source of Wealth (SoW) were generated from a sanctioned activity;
 - Clients whose source of funds (SoF) and source of Wealth (SoW) cannot be verified when this is required;
 - Purchase or sale of virtual assets ultimately owned or controlled, directly or indirectly, by sanctioned parties;
 - Transactions with third parties ultimately owned or controlled, directly or indirectly, by sanctioned parties;
- h. Establish a business relationship and/or conduct transactions with natural or legal persons residing in a jurisdiction/country where it is prohibited by Company policy to offer its services to. Prohibited jurisdictions / countries shall include:

Unrecognised / Disputed Territories

Crimea	Republic of Abkhazia
Donetsk	Republic of China (Taiwan)
Luhansk	Republic of Kosovo
Nagorno Karabakh Republic	Republic of Somaliland
Palestine	Republic of South Osetia
Pridnestrovian Moldavian Republic	Turkish Republic of Northern Cyprus

Prohibited Jurisdictions / Countries

Australia	Libya
Belarus	Mali
Belize	Netherlands
Central African Republic	North Korea
Cuba	Russia
Curaçao	Somalia
Democratic Republic of Congo	Sudan
Dutch West Indies (Aruba, Bonaire)	Syria
France	Turkish Republic of Northern Cyprus
Germany	UK
Iran	USA
Iraq	Yemen
Lebanon	Libya

8. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) procedures are applied to customers who present an elevated risk profile. This includes Politically Exposed Persons (PEPs), their family members, and close associates; customers based in or funding their accounts from high-risk jurisdictions; those conducting unusually large, complex, or unexplained transactions; and customers whose financial behaviour is inconsistent with their declared income or business activities.

EDD involves a more detailed and rigorous verification process than standard due diligence. This includes a full analysis of the customer's source of funds and source of wealth, supported by credible and independent documentation. Additional steps include corporate registry and public record searches to verify legal and beneficial ownership, confirmation of employment or business ownership, reviews of audited financial statements or other reliable financial documents, and thorough adverse media and reputational checks.

Senior management approval is required before onboarding any high-risk customer, and in complex or sensitive cases, formal approval from the Board of Directors may be necessary.

Once these customers are onboarded, they are subject to ongoing enhanced monitoring. This includes lower thresholds for triggering transaction reviews, closer scrutiny of their transaction patterns, and more frequent reassessments of their risk profiles. These measures ensure that higher-risk relationships are managed appropriately, in full alignment with both regulatory obligations and the company's internal risk appetite.

Prohibited Customer Categories

Luckyroo N.V. will not onboard or will immediately terminate relationships with customers who meet any of the following criteria:

- Anonymous or unverifiable customers, including those who fail or refuse identity verification within 30 days.
- Shell companies, fictitious entities, or customers with unclear beneficial ownership.
- Sanctioned individuals or entities, including those appearing on UN, EU, OFAC, OFSI, SNO, or Kingdom Sanction Act lists.
- Residents of or transacting from prohibited or sanctioned jurisdictions, as defined in Section 4 (Geographic Risk).
- Customers below the legal age for gambling.
- Customers involved in fraud, bonus abuse, identity theft, or other illicit behaviour.
- Third-party transactors or users of anonymous payment channels without valid justification or verification.
- Customers whose source of funds or source of wealth cannot be verified or is linked to crime.

Acceptance and Rejection Triggers

Customer applications will be immediately rejected or suspended when any of the following triggers occur:

a. Documentation and Verification Failures

- Refusal to provide KYC, proof of address, or EDD documentation.
- Submission of false, altered, or misleading information.
- Failure to complete mandatory verification within 30 days.

b. AML/CTF/CPF Risk Triggers

- Positive sanctions match or verified PEP hit without manageable risk.
- Suspicion of money laundering, terrorist financing, proliferation financing, or other criminal activity.
- Inability to verify SOF/SOW after reasonable attempts.

c. Behavioural and Transactional Triggers

- Highly unusual deposit/withdrawal activity inconsistent with profile.
- Multiple accounts, third-party payments, or misuse of payment instruments.
- Attempts to circumvent controls or operate through intermediaries.
- Evidence of collusion, chip dumping, or non-genuine gameplay.

9. Termination

Luckyroo N.V. reserves the right to suspend or terminate any customer relationship when required by regulations, internal policies, or risk considerations. This action may be taken if a customer fails to provide the requested identification or supporting documentation within 30 calendar days, if there is reasonable suspicion of money laundering, terrorist financing, or proliferation financing, or if the customer engages in activities that violate applicable laws, regulations, or the company's Responsible Gambling Policy.

When a relationship is terminated due to suspected criminal activity, the company promptly files a report with the Financial Intelligence Unit (FIU) in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Any remaining funds in the account are returned to the original funding source unless there is a legal requirement to freeze or seize the funds pending investigation. Detailed records of all termination actions, including the rationale and supporting evidence, are maintained for at least five years.

Luckyroo N.V. will refuse to onboard or will terminate an existing relationship in cases where:

- The customer is a resident of, located in, or conducting transactions from a prohibited or sanctioned jurisdiction.
- The customer fails to provide required information or documentation within the specified timeframe.
- False, misleading, or incomplete information is provided during registration or verification.
- The source of funds or source of wealth cannot be confirmed as legitimate.
- The customer is involved in, or suspected of, money laundering, terrorist financing, or other criminal activity.
- The customer is a Politically Exposed Person (PEP) whose risk profile cannot be mitigated to an acceptable level.
- Fraudulent activities, bonus abuse, collusion, or prohibited gambling behaviour are detected.
- The customer attempts to use third parties to transact without proper disclosure and verification.
- The customer has self-excluded or been excluded for responsible gambling reasons.
- Large chip redemptions or withdrawals are requested without verifiable linked gambling activity.
- The customer is a minor or below the legal gambling age in their jurisdiction.

10. Curaçao's Legislative Framework

Luckyroo N.V. acknowledges that its Customer Acceptance Policy is an integral part of its wider Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) framework. The policy is designed to fully comply with Curaçao's legal and regulatory requirements, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

Compliance with these obligations is treated as a priority in daily operations. The customer acceptance procedures are embedded within the company's compliance processes to ensure due diligence is continuous and extends beyond onboarding. This approach ensures that any significant changes in a customer's risk profile, transactional behaviour, or jurisdiction are identified and addressed promptly.

All employees involved in onboarding and verification activities receive dedicated training to help them understand the legislative framework and the company's internal standards. The training focuses on effectively applying the Risk-Based Approach, identifying and escalating high-risk indicators, and following escalation protocols to the Compliance Officer or senior management.

Independent audits are conducted at least annually to evaluate how effectively the Risk-Based Approach and the Customer Acceptance Policy are being implemented. These audits review critical processes, such as identity verification, sanctions and PEP screening, Enhanced Due Diligence (EDD) procedures, and the ongoing monitoring of customer activities. The findings are reported to the Board of Directors, and any gaps or deficiencies are addressed promptly through corrective measures implemented within defined timeframes.

11. Responsible Gambling Integration

Luckyroo N.V. ensures that its Customer Acceptance Policy is fully aligned with its Responsible Gambling Policy, recognising that protecting customers from gambling-related harm is a key part of its compliance and operational framework.

If a customer shows behaviour that indicates potential harm, such as frequent deposits that exceed their apparent financial capacity or excessively long gaming sessions, the company takes immediate action. Depending on the situation, this may include setting deposit or wagering limits, temporarily suspending the account, or, in severe cases, refusing further access to services to protect the customer.

Self-exclusion requests are handled promptly and applied to all accounts linked to the customer to ensure these measures cannot be bypassed. These restrictions remain active for the period specified by the customer or as required by regulatory standards.

Employees in customer-facing roles receive targeted training to help them identify early signs of problem gambling. This training is incorporated into both the onboarding process and ongoing monitoring activities, enabling timely intervention when risk indicators are observed.

12. Review and Governance of CAP

This Customer Acceptance Policy (CAP) is reviewed at least once every twelve months to ensure that it remains effective, compliant with legislative and regulatory requirements, and consistent with industry best practices. The review process also takes into account any changes to the company's risk profile, emerging patterns in customer behaviour, and technological advancements that could create new risks or vulnerabilities.

Proposed revisions or updates are prepared by the Compliance Officer and submitted to the Board of Directors for approval prior to implementation. All updates are thoroughly documented, and relevant staff are informed and trained to ensure that the revised policy is applied consistently and accurately throughout the company's operations.

13. Record Keeping

Luckyroo N.V. keeps detailed records of all customer acceptance activities for at least five years after the end of the business relationship, in accordance with regulatory requirements. These records include identification and verification documents, proof of address, evidence of the source of funds and source of wealth, transaction monitoring alerts and investigation reports, Enhanced Due Diligence (EDD) files, internal compliance reviews, and documentation of any account suspensions or terminations.

All records are stored securely in encrypted formats with strict access controls to ensure confidentiality and data protection. Only authorised personnel have access to these records, and all access activity is logged and periodically reviewed to verify compliance with internal policies and applicable data protection regulations.