

Anti-Money Laundering and Countering Financial Crime Manual (AML/CFT)

Zenith Crest B.V.

Version 1.0 / January 2025

Document Control

- **Version:** 1.0
- **Effective Date:** January 1st, 2025
- **Last Revision:** Initial Version
- **Next Review:** January 1st, 2026
- **Approval:** Board of Directors & MLRO

Glossary of Terms

- **AML/CFT:** Anti-Money Laundering and Countering the Financing of Terrorism
- **MLRO:** Money Laundering Reporting Officer
- **B2B:** Business-to-Business
- **CDD:** Customer Due Diligence
- **EDD:** Enhanced Due Diligence
- **FATF:** Financial Action Task Force
- **CGA:** Curaçao Gaming Authority
- **PEP:** Politically Exposed Person
- **SOF:** Source of Funds
- **STR:** Suspicious Transaction Report

1. Purpose of the AML/CFT Manual & Objectives

1.1 Purpose of the AML/CFT Manual

This manual aims to:

- Provide clear guidance to staff, Directors, and relevant authorities on the responsibilities of Zenith Crest B.V., a gaming software distributor incorporated in Curaçao, registration number 165208, with its address at Zuikertuinitjeweg Z/N, Curaçao.
- Offer a comprehensive overview of the internal policies and procedures established to ensure compliance with these responsibilities.

To meet legal obligations, this manual aligns with:

- **Curaçao:** National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (Landsverordening bestrijding witwassen en terrorismefinanciering), regulated by the Curaçao Gaming Authority (CGA).
- **EU:** Directive 2015/849 and Regulation 2015/847, which enforce AML/CFT standards across member states, as applicable to Curaçao's international commitments.

The manual outlines internal measures, policies, and procedures designed to fulfill licensing and operational requirements, establishing a robust compliance framework.

1.2 Policy Statement and Objectives

Zenith Crest B.V. is firmly committed to ensuring that all staff and Directors actively work to prevent the misuse of our services by criminals or terrorists for money laundering or terrorist financing. The objectives of this commitment include:

- Achieving full compliance with all relevant laws, regulations, and requirements set by authorities in Curaçao and the EU.
- Protecting Zenith Crest B.V., its staff, and Directors from risks associated with breaches of legal and regulatory standards.
- Minimizing reputational harm from money laundering or terrorist financing by contributing meaningfully to combating financial crime.

To achieve these goals, Zenith Crest B.V.'s policy mandates:

- Staff and Directors must be fully aware of and comply with their personal legal obligations related to their roles within the company.
- Commercial interests or decisions must never take precedence over Zenith Crest B.V.'s commitment to preventing money laundering, terrorist financing, or other financial crimes.
- A Money Laundering Reporting Officer (MLRO) must be appointed, and all staff are required to provide full support and cooperation in fulfilling the duties of this role.

- Zenith Crest B.V. will not knowingly establish or continue B2B relationships with entities, corporations, or businesses suspected of engaging in illicit or unethical activities.
- Zenith Crest B.V. will not knowingly accept payments or funds from B2B relationships with entities suspected of such activities.

2. Background to Money Laundering and Terrorist Financing

Zenith Crest B.V. is dedicated to preventing and deterring the misuse of its B2B gaming software distribution services by criminals and terrorists. Curaçao and the European Union uphold global standards to combat money laundering and terrorist financing, and Zenith Crest B.V. has implemented policies and procedures to detect and prevent potential abuse of our platform.

2.1 What is Money Laundering?

Money laundering involves any process or activity that disguises the origins of funds or property derived from criminal activities, making them appear legitimate. It occurs whenever illicit proceeds are involved. The primary goals of money launderers are:

- To hide the criminal origins of their proceeds.
- To retain control over these funds while obscuring their ownership.
- To evade detection by law enforcement or regulatory authorities.
- To ultimately profit from the illicit gains.

Money laundering typically involves three stages:

- **2.1.1 Placement:** This initial stage introduces criminal proceeds into the financial system. For Zenith Crest B.V., as a B2B gaming software distributor, placement could occur if unethical gaming operators use illicit funds to purchase our software licenses, inadvertently involving us in the laundering process as these funds enter legitimate financial channels.
- **2.1.2 Layering:** This stage involves multiple transactions to distance the proceeds from their entry point, obscuring their trail and creating an appearance of legitimacy. In our context, layering might involve multiple B2B clients with minimal trading history engaging with Zenith Crest B.V. or operators reporting unusually high player activity shortly after onboarding, creating complex layers to hinder investigations.
- **2.1.3 Integration:** The final stage reintegrates laundered funds into the legitimate economy, appearing as lawful earnings. For Zenith Crest B.V., this could involve routine payments for software services that originate from earlier laundering efforts. Vulnerabilities, such as cross-border payments or asset purchases, may provide opportunities for authorities to detect such activities.

Money laundering may not always follow a clear three-stage process; stages can overlap, and the process may involve various forms of property beyond cash. Given the high-value nature of contracts in the gaming software industry, Zenith Crest B.V. must remain vigilant throughout each B2B relationship to prevent misuse.

2.2 What is Terrorist Financing?

The United Nations Convention for the Suppression of the Financing of Terrorism defines terrorism as actions intended “to intimidate a population, or to compel a government or an international organization to do or abstain from doing any act.” It prohibits anyone from

directly or indirectly handling or providing funds with the intent or knowledge that they will support terrorist acts or groups.

- **2.2.1 Terrorism Factors:** Terrorist activities typically involve:
 - Threats or acts aimed at influencing governments or intimidating the public, often for political, religious, or ideological purposes.
 - Actions causing serious violence, significant property damage, or endangering lives to advance these goals.
 - Criminal enterprises generating consistent income for terrorist organizations.
- **2.2.2 Financial Support of Terrorism:** Funding for terrorism typically comes from:
 - “State-sponsored terrorism,” where nations, organizations, or wealthy individuals provide resources to terrorist causes, though this has declined due to international efforts.
 - Revenue-generating activities, both legal and illegal, conducted by terrorist groups, often targeting high-profit ventures to sustain operations.

Staff and Directors of Zenith Crest B.V. must exercise heightened caution when engaging with new B2B clients in jurisdictions known to have ties to terrorist organizations, as listed in Appendix 2.

2.3 Proliferation Financing

- **2.3.1 What is Proliferation?:** Per UN Security Council Resolution 1540, proliferation refers to “the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, or use of chemical, biological, radiological, or nuclear (CBRN) weapons (weapons of mass destruction or WMD) and their delivery systems or related materials (including technologies and dual-use goods), in violation of national laws or international commitments.” This includes advanced missile systems and rudimentary devices like “dirty bombs.”
- **2.3.2 Dual-Use Goods:** These are items with legitimate uses that can also be repurposed for proliferation activities, such as WMD development. In Zenith Crest B.V.’s case, our gaming software could theoretically be misused, despite its primary lawful purpose. Such goods may not appear on control lists, necessitating careful client assessments. Without proper controls, these materials could reach unauthorized parties, profiteers, or terrorists, posing a global security threat.
- **2.3.3 Proliferation Financing:** The Financial Action Task Force (FATF) defines proliferation financing as “the act of providing funds or financial services used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including technologies and dual-use goods for non-legitimate purposes), in contravention of national laws or international obligations.” This includes:
 - Financing terrorism, where funds support groups seeking WMD.
 - State-backed efforts to develop or enhance WMD capabilities.

Proliferation financing often mimics legitimate transactions to access foreign currency or the global financial system, making scrutiny of payment chains critical. Even unintentional involvement risks severe reputational damage, emphasizing the need for robust preventive measures.

2.4 Sanctions

Sanctions are punitive measures imposed on countries, individuals, entities, or organizations to maintain or restore international peace and security. These target specific sectors, industries, or persons and are guided by lists from the United Nations (UN), European Union (EU), and the U.S. Office of Foreign Assets Control (OFAC). Zenith Crest B.V., incorporated in Curaçao, adheres to international sanctions and voluntarily complies with OFAC measures, including:

- Prohibiting business with individuals or entities from OFAC-sanctioned jurisdictions such as Iran, North Korea, and Myanmar (see Appendix 2).
- Monitoring OFAC's "Specially Designated Nationals and Blocked Persons List," "Sectoral Sanctions Identifications List," and programs like "Counter Terrorism" and "Non-Proliferation."

Sanctions may involve:

- Freezing assets and prohibiting resource provision to designated parties.
- Economic restrictions on specific businesses or sectors.
- Controls on dual-use goods, arms embargoes, and import/export bans.
- Travel or visa restrictions for targeted individuals.

If a B2B client or its Ultimate Beneficial Owner (UBO)/Directors is identified as a sanctioned entity or individual (per Appendix 2), staff must immediately compile a full client profile, halt all transactions, and notify the MLRO, who will escalate to the relevant authorities. Zenith Crest B.V. maintains a PEP and Sanctions Register to record such cases.

3. Legal and Regulatory Compliance Framework

This section outlines the legislative and regulatory requirements that Zenith Crest B.V., a gaming software distributor incorporated in Curaçao with registration number 165208, must follow. It provides an overview of laws governing anti-money laundering (AML), countering the financing of terrorism (CFT), and related obligations under Curaçao and EU jurisdictions, where applicable. While not exhaustive, this section equips staff and Directors with essential knowledge of the legal landscape, their responsibilities, and the consequences of non-compliance. Staff are encouraged to consult referenced legislation or seek clarification from the MLRO for full details.

3.1 Curaçao AML/CFT Legislation

Curaçao's primary legal framework for combating money laundering and terrorist financing is the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing. This aligns with international standards and applies to Zenith Crest B.V. Key offenses include:

- Concealing, transferring, or disguising criminal proceeds to obscure their illicit origins.
- Assisting another individual or entity in retaining or benefiting from criminal proceeds.
- Acquiring, possessing, or using property known or suspected to be derived from crime.

Penalties:

- Conviction for these offenses may result in up to 7 years imprisonment.
- Failing to report knowledge or suspicion of money laundering to the MLRO or authorities carries a penalty of up to 4 years in custody.
- Tipping off—disclosing information likely to prejudice an investigation—may lead to up to 2 years imprisonment.

All staff and Directors have a legal duty to report any suspicion or knowledge of money laundering encountered during their work to the MLRO immediately. Criminal conduct includes acts that would be offenses under Curaçao law or, if committed abroad, would constitute crimes if they occurred in Curaçao.

3.2 Curaçao Gaming and AML Legislation

The Curaçao gaming regulations, overseen by the Curaçao Gaming Authority (CGA), mandate AML/CFT compliance for gaming software distributors, requiring robust measures to prevent misuse of our services. Offenses include:

- Facilitating transactions involving criminal proceeds through gaming-related activities.
- Failing to implement required due diligence or reporting procedures.

Penalties:

- Non-compliance may result in fines, license suspension, or revocation, halting operations.
- Criminal involvement in money laundering or terrorist financing may lead to imprisonment under Curaçao penal law, with terms up to 7 years depending on severity.

3.3 EU Directives and Regulations

Zenith Crest B.V. adheres to the EU framework, where applicable, including:

- **Directive 2015/849 (4th AML Directive):** Establishes a risk-based approach to prevent money laundering and terrorist financing, requiring customer due diligence, record-keeping, and suspicious activity reporting. Non-compliance risks fines or sanctions from regulators.
- **Regulation 2015/847:** Ensures transparency in fund transfers, requiring traceability of payments linked to our B2B contracts. Violations may lead to regulatory penalties.

These EU laws reinforce our obligations within Curaçao's international compliance framework.

3.4 Terrorist Financing Laws

Terrorist financing is addressed under Curaçao legislation, aligned with the UN Convention for the Suppression of the Financing of Terrorism and, where applicable, EU Directive 2015/849. Offenses include:

- Providing, collecting, or making available funds with intent or knowledge that they will support terrorist acts or organizations.
- Concealing or transferring property known to be linked to terrorism.
- Arranging financial resources suspected to be used for terrorist purposes.

Penalties:

- Conviction carries imprisonment of up to 7 years in Curaçao.
- Failure to report suspicion or knowledge of terrorist financing to the MLRO or authorities is punishable by up to 4 years in custody.

Staff must escalate concerns arising from B2B client activities to the MLRO without delay.

3.5 Sanctions Compliance Obligations

Zenith Crest B.V. complies with sanctions imposed by the UN and voluntarily adheres to U.S. OFAC measures, as well as EU sanctions where applicable. These include:

- Prohibitions on dealings with sanctioned individuals, entities, or jurisdictions (e.g., Iran, DPRK).
- Restrictions on financial services or goods transfers that could breach sanctions.

Penalties:

- Breaching sanctions may result in fines, asset freezes, or operational bans enforced by authorities.
- Non-compliance with OFAC (though voluntary) risks reputational damage and exclusion from U.S.-linked financial systems.

3.6 Staff Responsibilities and Consequences

Every staff member and Director has a personal legal obligation to:

- Understand and comply with the AML/CFT requirements outlined in this manual.
- Report any suspicion or knowledge of money laundering, terrorist financing, or sanctions breaches to the MLRO immediately, following Section 7 procedures.
- Avoid actions that could constitute tipping off, such as alerting a client to an investigation.

Failure to meet these duties is a criminal offense, exposing individuals to imprisonment or fines, separate from company-level penalties. Staff with questions should consult the MLRO for guidance.

3.7 Additional Regulatory Guidance

The FATF Recommendations (2012), incorporated into Curaçao laws, provide international standards that Zenith Crest B.V. follows, including risk-based customer due diligence and enhanced measures for high-risk scenarios. Compliance is monitored by authorities to ensure alignment with global best practices.

4. Customer Dose Diligence and Risk Assessment

Zenith Crest B.V., as an ethical B2B gaming software distributor, adopts a comprehensive risk-based approach (RBA) to assess and monitor business clients, mitigating risks of money laundering (ML), terrorist financing (TF), proliferation financing (PF), and other financial crimes. This section outlines the criteria, processes, and controls to safeguard our operations under Curaçao and EU legislation.

4.1 Risk Assessment Criteria

We evaluate B2B clients based on multiple factors to determine their risk level:

- **Payment Behavior:** Irregular or frequent payment requests deviating from agreed terms may indicate layering attempts. Consistent payments align with lower risk.
- **Geographic Location:** Clients in high-risk jurisdictions (Appendix A) with weak AML/CFT controls or ties to crime/terrorism increase risk. Clients in low-risk, FATF-compliant jurisdictions are generally safer but still require scrutiny.
- **Source of Funds (SOF):** Unclear, non-FATF, or high-risk jurisdiction funds raise suspicion. Verified, legitimate SOF reduces risk.
- **Client Profile and Ownership:** PEPs, sanctioned individuals, or entities with adverse media in the ownership structure elevate risk. Transparent, reputable businesses pose lower risk.

Risk Categories:

- **Standard Risk:** Clients from standard-risk jurisdictions with clear SOF and stable operations.
- **High Risk:** Clients with PEPs, high-risk jurisdiction ties, or suspicious patterns, requiring enhanced due diligence (EDD).

4.2 Initial Client Onboarding Process

Before establishing a B2B relationship, Zenith Crest B.V. conducts thorough due diligence:

- **Documentation:** Clients provide company registration details, beneficial owner (UBO) identification, and initial SOF evidence.
- **Screening:** The Compliance Unit screens UBOs and Directors against PEP and sanctions lists using appropriate tools. Positive hits are escalated to the MLRO.
- **Blacklist Check:** Clients are cross-referenced against an internal blacklist of terminated or suspicious entities maintained by the MLRO.
- **Approval:** Contracts are finalized only after Compliance Unit clearance, with high-risk cases requiring MLRO approval.

4.3 Enhanced Due Diligence (EDD) for High-Risk Clients

EDD is mandatory for high-risk clients:

- **Triggers:**

- Location in high-risk jurisdictions (Appendix A).
- UBOs or Directors identified as PEPs or sanctioned persons.
- Unverifiable SOF or links to high-risk sources.
- **Requirements:**
 - Certified copies of UBO identification.
 - Recent proof of address.
 - Detailed SOF documentation.
- **Process:** The Compliance Unit compiles a risk dossier, reviewed by the MLRO. Services are paused until EDD is completed and approved.

4.4 Ongoing Monitoring and Review

Zenith Crest B.V. maintains continuous oversight of B2B relationships:

- **Annual Assessment:** The Data Analytics Team compares payment volumes and player activity against onboarding projections, flagging deviations.
- **Automated Tools:** Software monitors transaction frequency and volume, alerting the Compliance Unit to anomalies.
- **Manual Review:** The Compliance Unit investigates flagged cases, requesting client explanations. Unresolved issues escalate to the MLRO for EDD or termination.
- **Frequency:** High-risk clients are reviewed semi-annually; standard-risk clients annually.

4.5 Contractual Obligations and Restrictions

B2B contracts enforce AML/CFT compliance:

- Clients must warrant software use complies with local gaming laws and restricts play to individuals aged 18 or older.
- Non-compliance triggers immediate service suspension, pending Compliance Unit investigation.
- Periodic audits verify adherence, conducted by Operational Staff under MLRO oversight.

4.6 Source of Funds Verification

For high-risk contracts:

- **Evidence:** Clients submit financial statements, bank records, or ownership documents proving legitimate funding.
- **Validation:** The Compliance Unit cross-checks against independent sources.
- **Escalation:** Unverifiable SOF halts services until resolved, with the MLRO deciding on termination if suspicion persists.

4.7 Internal Record Management

- **Updates:** Client detail changes are logged and reviewed by the MLRO within 48 hours.
- **Storage:** Due diligence records are encrypted and stored for 10 years post-relationship, accessible only to authorized personnel.

- **Blacklist:** Terminated high-risk clients are added to an internal blacklist, securely maintained by the MLRO.

5. Technology and Innovation Risk Management

Zenith Crest B.V. acknowledges that new products, business practices, or technologies in our B2B gaming software distribution may create vulnerabilities exploitable by money launderers, terrorist financiers, or proliferators. This section outlines procedures to assess and manage these risks, ensuring compliance with Curaçao and EU legislation while fostering responsible innovation.

5.1 Pre-Launch Risk Assessment

Before deploying new software, services, or technological enhancements, Zenith Crest B.V. conducts a thorough AML/CFT risk assessment:

- **Responsibility:** The Data Analytics Team, under MLRO oversight, leads the evaluation, collaborating with Operational Staff to analyze technical specifications.
- **Scope:** The assessment examines potential vulnerabilities that could facilitate financial crime.
- **Methodology:** Risks are rated (low, medium, high) based on likelihood and impact, using historical data, industry benchmarks, and FATF guidance.
- **Documentation:** A detailed risk report identifies vulnerabilities and exploitation scenarios, submitted to the MLRO.

5.2 Risk Mitigation Strategies

Upon identifying risks, Zenith Crest B.V. implements tailored controls:

- **Testing:** Controls are stress-tested in a sandbox environment, simulating ML/TF scenarios to confirm effectiveness.
- **Timeline:** Mitigation plans are finalized, with progress tracked via a project log maintained by the Data Analytics Team.

5.3 Implementation and Approval

Once risks are mitigated, the new technology or product moves to implementation:

- **Rollout:** Operational Staff deploy the technology, with initial use monitored for unforeseen issues.
- **Training:** Staff receive targeted AML/CFT training on the new system, delivered by the MLRO prior to launch.

5.4 Post-Launch Monitoring

After deployment, Zenith Crest B.V. ensures ongoing vigilance:

- **Regular Audits:** The Compliance Unit conducts quarterly reviews of technology performance, assessing metrics like false positive rates or security incidents.
- **Feedback Loop:** Operational Staff report anomalies to the Data Analytics Team, triggering re-assessment if needed.

- **Updates:** Software patches or procedural adjustments are implemented under MLRO oversight.

6. Record Retention and Management

Zenith Crest B.V. maintains meticulous records of B2B client interactions, transactions, and due diligence to comply with legislative requirements. This section outlines policies for retaining, retrieving, and securing records to support audits, regulatory inquiries, and investigations.

6.1 Retention Obligations

- **Duration:** Records related to client relationships and transactions are retained for a minimum period post-relationship or final transaction, including identification documents, SOF evidence, payment records, and risk assessments.
- **Scope:** Retention covers active and terminated B2B relationships, including onboarding data, monitoring logs, and correspondence.

6.2 Storage Protocols

- **Formats:** Records are maintained in electronic and hard copy formats for redundancy and accessibility.
- **Security:** Electronic records are stored on encrypted servers with industry-standard protocols.
- **Backup:** Regular backups of electronic records are performed.

7. Suspicious Activity Reporting and Internal Controls

Zenith Crest B.V. maintains a robust internal reporting system to detect and address potential ML, TF, or PF risks from our B2B gaming software distribution activities. This section outlines procedures for staff to recognize suspicious transactions, report to the MLRO, and ensure compliance with Curaçao and EU legislation.

7.1 Money Laundering Reporting Officer (MLRO)

- **Designation:** Zenith Crest B.V. appoints an MLRO to oversee AML/CFT compliance. The current MLRO is Philip Bugeja.
- **Contact Details:**
 - **Address:** Zuikertuinitjeweg Z/N, Curaçao
 - **Email:** philip@igagroup.com
- **Responsibilities:**
 - Receive and assess internal suspicious activity reports.
 - Investigate suspicions and determine if external reporting to authorities is required.
 - Oversee daily client account activities and high-risk cases.
 - Ensure access to necessary systems, files, and documents for thorough evaluations.

The MLRO is supported by all staff, who must cooperate fully.

7.2 Recognizing Suspicious Activities

Staff are trained to identify unusual or suspicious activities, such as:

- Revenue patterns inconsistent with onboarding projections.
- Unverifiable or overly complex SOF.
- Client behavior indicating secrecy or intent to conceal transactions.
- Difficulty explaining business operations or lack of industry knowledge.
- Funds linked to high-risk ML/TF jurisdictions (Appendix A).

Staff must document concerns and follow the reporting process.

7.3 Internal Reporting Process

- **Obligation:** Staff must report suspicions of ML, TF, or PF to the MLRO promptly using the Internal Suspicion Report Form (Appendix B). Failure to report is a criminal offense under Curaçao law.
- **Submission:**
 - Complete the Internal Suspicion Report Form with detailed suspicion and evidence.
 - Submit to the MLRO via secure email or in-person within 24 hours.
- **Content:** Reports must be clear, legible, and comprehensive.
- **Tipping Off Prohibition:** Staff must not disclose suspicions to clients or third parties, as this could prejudice investigations and is punishable by imprisonment.

- **Clarification:** The MLRO may request additional client information discreetly, with findings forwarded for evaluation.

7.4 MLRO Review and Decision-Making

- **Receipt:** The MLRO acknowledges reports within 24 hours, logging them in the Internal Suspicion Register.
- **Investigation:** The MLRO reviews reports, accessing client records and due diligence files, completing assessments within 5 business days.
- **Outcome:**
 - If unfounded, the MLRO documents the rationale and closes the case, informing staff.
 - If suspicion persists, the MLRO prepares an external report for authorities.
- **Record-Keeping:** Decisions and documents are archived securely, with outcomes noted in the Internal Suspicion Register.

7.5 Management of Registers

- **Internal Suspicion Register:**
 - Tracks reports, including submission date, staff name, client details, MLRO decision, and closure date.
 - Reviewed monthly by the MLRO for trends.
- **External Disclosure Register:**
 - Logs STRs filed with authorities, noting submission date, reference numbers, and acknowledgments.
 - Kept secure with access restricted to the MLRO.
- **External Enquiries Register:**
 - Records inquiries from authorities, detailing date, officer, legal basis, and information provided.
 - Maintained indefinitely, with destruction only upon regulatory approval.

7.6 Staff Accountability and Legal Consequences

- **Duty:** Staff must understand their legal obligation to report suspicions, as failure risks personal penalties, including imprisonment.
- **Support:** The MLRO provides guidance on reporting procedures.
- **Confidentiality:** Reporting is handled discreetly, protecting staff while maintaining investigation integrity.

8. Staff Recruitment, Training, and Compliance Oversight

Zenith Crest B.V. recognizes that staff and Directors are critical to maintaining a robust AML/CFT framework. This section outlines policies for screening, training, and overseeing personnel to ensure expertise, integrity, and awareness to prevent financial crime.

8.1 Staff Recruitment and Screening

- **Objective:** Ensure employees uphold honesty and trustworthiness to reduce internal fraud or criminal facilitation risks.
- **Process:**
 - Background checks verify identity, employment history, and criminal records.
 - References from previous employers are authenticated by the HR Unit.
 - Senior staff undergo enhanced screening.
- **Documentation:** Screening results are recorded in secure personnel files, accessible only to HR and the MLRO, retained as required by law.
- **Outcome:** Candidates failing integrity standards are excluded, with decisions logged for audits.

8.2 AML/CFT Training Program

- **Purpose:** Equip staff with knowledge to recognize and report suspicious activities.
- **Frequency:**
 - Initial training upon onboarding, with annual refreshers.
 - Additional training for legal, policy, or technology updates.
- **Content:**
 - ML, TF, and PF risks in gaming software distribution.
 - Responsibilities and legal consequences of non-compliance.
- **Delivery:**
 - Led by the MLRO, conducted in-person or via secure virtual platforms.
 - Materials, including this manual, are distributed electronically, with written acknowledgment required.
- **Assessment:** Periodic quizzes verify comprehension.

8.3 Ongoing Compliance Monitoring

- **Responsibility:** The HR Unit, with the MLRO, oversees staff adherence.
- **Tracking:**
 - Training completion is recorded in a secure register, reviewed quarterly by the MLRO.
 - Staff performance in reporting is monitored, with feedback provided.
- **Audits:** The Compliance Unit conducts semi-annual reviews of staff compliance, reporting findings to the Board.
- **Updates:** Legal or procedural changes are communicated promptly, with retraining scheduled.

8.4 Support and Guidance

- **Resources:** Staff have access to the MLRO for clarification, with timely responses.
- **Escalation:** Complex issues are escalated to senior management or external advisors, with resolutions documented.
- **Continuous Improvement:** Feedback from training and reviews refines programs.

9. Supporting Appendices

This section provides reference materials to support Zenith Crest B.V.'s AML/CFT policies and procedures. These appendices assist staff and Directors in understanding risk classifications, definitions, and documentation requirements.

9.1 Appendix 1 - Acceptable Jurisdictions

- **Purpose:** Identifies low or medium-risk jurisdictions for business dealings, based on adherence to international AML/CFT standards.
- **Criteria:** Jurisdictions must have robust legal frameworks equivalent to Curaçao's, with no significant ML/TF risks per FATF.
- **List:**

Risk Level	Countries
Low Risk	Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Norway, Poland, Romania, Slovakia, Slovenia, Sweden, Japan, New Zealand, Singapore, Switzerland
Medium Risk	Bulgaria, Croatia

- **Updates:** Reviewed quarterly by the MLRO, with revisions approved by the Board.

9.2 Appendix 2 - Unacceptable and High-Risk Jurisdictions

- **Purpose:** Identifies jurisdictions where business is restricted or requires enhanced scrutiny due to elevated ML/TF/PF risks.
- **Criteria:** Based on FATF designations (February 2025), including jurisdictions under increased monitoring or countermeasures.
- **Classifications and List:**

Risk Level	Countries
Medium Risk	Algeria, Angola, Burkina Faso, Cameroon, Côte d'Ivoire, Democratic Republic of the Congo, Haiti, Kenya, Lao PDR, Lebanon, Mali, Monaco, Mozambique, Namibia, Nepal, Nigeria, South Africa, South Sudan, Syria, Tanzania, Venezuela, Vietnam, Yemen
High Risk	Democratic People's Republic of Korea, Iran, Myanmar

- **Application:** High-risk jurisdictions trigger mandatory EDD; business with unacceptable jurisdictions is prohibited unless approved by the MLRO and Board.
- **Maintenance:** Updated quarterly by the MLRO, aligned with FATF and EU/OFAC sanctions lists.

9.3 Appendix 3 - Politically Exposed Persons (PEPs) and High-Risk Customers (HRCs)

- **Definitions:**
 - **PEPs:** Individuals in prominent public positions, their family members, or close associates, including heads of state, ministers, senior judicial/military officials, and state-owned entity executives.
 - **HRCs:** Customers or beneficial owners posing elevated ML/TF risks due to jurisdictional ties, adverse media, or complex ownership.
- **Identification:** Flagged during onboarding and monitoring via screening tools and risk assessments.
- **Handling:** Both require EDD, with records maintained in a dedicated register by the MLRO.

9.4 Appendix 4 - Internal Suspicion Report Form

- **Purpose:** Standardizes reporting of suspicious activities.
- **Template:**
 - Date Submitted:
 - Staff Name:
 - Client Name:
 - Suspicion Details:
 - Evidence:
- **Use:** Completed by staff upon identifying suspicious activity, submitted to the MLRO.
- **Retention:** Stored securely with client records, per Section 6 requirements.