

# **AZRA 678 KNOW YOUR CUSTOMER (KYC) POLICY**

## **Table of Contents**

1. Purpose and scope
2. Definitions
3. Responsibilities and governance
4. Timing of customer due diligence
5. Documents and information requested
6. Customer due diligence criteria and risk scoring
7. Threshold procedure XCG 4,000
8. Missing documents at threshold and 30-day follow up
9. Ongoing monitoring and red flags
10. Politically Exposed Persons screening and EDD
11. Sanctions screening, freezing and reporting
12. Account restrictions, suspension and termination
13. Recordkeeping and retention
14. Training, audit and review
15. Annexes and templates

Annex 1: Onboarding Checklist

Annex 2: XCG 4,000 Operational Flowchart

Annex 3: PEP Declaration Form Annex 4 SoF / SoW Evidence Template

Annex 5: 30-day Reminder & Termination Email Templates

Annex 6: Escalation Matrix and SLAs

Annex 7: SAR Internal Template & FIU Checklist

Annex 8: KYC Case File Log Template

Annex 9: Device IP & Linkage Investigation Checklist

Annex 10: Policy Change Log

## 1. PURPOSE AND SCOPE

**Purpose:** Prevent, detect and report money laundering, terrorist financing and proliferation financing in line with Curaçao law and international standards.

**Scope:** This KYC Policy applies to all our brands, products, customer types, payment rails, internal counterparty relationships, and third-party service providers. It is a standalone KYC policy that complements the company AML/CFT/CFP Policy and operational procedures.

## 2. DEFINITIONS

- **Customer:** natural or legal person who opens an account or conducts an occasional transaction.
- **Beneficial owner:** natural person(s) who ultimately owns or controls a customer.
- **Occasional transaction:** single or linked transaction outside an established business relationship.
- **Politically Exposed Person (PEP):** as defined by Curaçao guidance and international standards.
- **Sanctions match:** confirmed positive identification against an applicable sanctions list.
- **Source of Funds (SoF):** origin of the funds used in a transaction.
- **Source of Wealth (SoW):** origin of the customer's overall wealth.
- **XCG 4,000:** operational threshold for enhanced due diligence (equivalent to USD 2,198 as used in internal policy references).
- **Risk categories:** Low / Medium / High.

## 3. RESPONSIBILITIES AND GOVERNANCE

- **Board of Directors:** ultimate responsibility for the AML/KYC framework and resourcing.
- **MLRO / AML Compliance Officer:** policy owner; responsible for suspicious transaction reporting to the FIU, sanctions escalation, regulatory liaison, and annual reporting to the Board.
- **KYC Team:** first-line execution of onboarding checks, document collection, identity verification, and initial risk scoring.
- **Operations and Payments:** enforce deposit/withdrawal blocks and payment-related holds per KYC decisions.
- **Senior Management:** approve onboarding or continuation of high-risk customers and PEP relationships; decide on termination where required.
- **Internal Audit:** periodic independent testing of KYC controls and remediation tracking.

All roles, responsibilities, and contact points are recorded in Annex 6 (Escalation Matrix).

#### 4. TIMING OF CUSTOMER DUE DILIGENCE

- **Initial CDD at account opening:** collect minimum personal details and perform sanctions & PEP screening before account activation.
- **Enhanced CDD:** required when cumulative customer activity reaches XCG 4,000, an occasional transaction equals or exceeds XCG 4,000, suspicion arises, or customer risk profile changes.
- **Event driven CDD:** triggered by adverse media, law enforcement request, payment provider alerts, or internal monitoring flags.
- **Ongoing CDD:** periodic refreshes and continuous transaction monitoring.

#### 5. DOCUMENTS AND INFORMATION REQUESTED

- **Minimum onboarding data (low risk):**
  - ✓ Full name;
  - ✓ Date of birth;
  - ✓ Permanent residential address;
  - ✓ Email and phone number;
  - ✓ Government issued photo ID;
  - ✓ Sanctions and PEP screening results.
- **Additional documents when required:**
  - ✓ High-quality color copy of passport or national ID;
  - ✓ Proof of address (utility bill or bank statement dated within 3 months);
  - ✓ Proof of payment method (bank statement, card verification);
  - ✓ SoF/SoW evidence (bank statements, payslips, sale agreements, tax returns);
  - ✓ Video KYC or certified documents where necessary.

**Document quality standards:** scanned color copies, legible, unexpired, and verified against independent sources. All documents are logged with verification date and verifier identity.

#### 6. CUSTOMER DUE DILIGENCE CRITERIA AND RISK SCORING

- **Risk factors considered:**
  - ✓ Jurisdiction risk;
  - ✓ Payment method risk (e.g., crypto or certain e-wallets flagged higher);
  - ✓ Transaction velocity and patterns;
  - ✓ PEP status;
  - ✓ Sanctions exposure;
  - ✓ Adverse media;
  - ✓ Account inconsistencies;

- ✓ Linked account indicators;
- ✓ Fraud indicators;
- ✓ Product or channel risk.
- **Risk categories:**
  - ✓ Low,
  - ✓ Medium,
  - ✓ High.
- **Scoring model:**
  - ✓ Automated baseline score from onboarding data and monitoring rules
  - ✓ Manual override by KYC analyst.
- **Risk reassessment** occurs on material changes or per scheduled refresh cadence:
  - ✓ Low 36 months;
  - ✓ Medium 24 months;
  - ✓ High 12 months or event-driven.
- **High risk triggers include:**
  - ✓ PEP status;
  - ✓ Confirmed adverse media linking to criminal activity;
  - ✓ Inability to verify identity;
  - ✓ Suspicious transaction patterns;
  - ✓ Jurisdictions subject to enhanced scrutiny.
- **Identification of Vulnerable Persons:**
  - ✓ As part of the Customer Due Diligence (CDD) process and in accordance with the National Ordinance on Games of Chance (LOK), Azra 678 performs specific checks to identify 'Vulnerable Persons.' A person is considered vulnerable if they fall into any of the following categories:
    - Minors: Any individual under the age of 18.
    - Gambling Addiction: Individuals who have declared a gambling addiction, those currently registered on a self-exclusion list, or those identified through behavioral monitoring as showing signs of problem gambling.
    - Legal Restraint: Individuals who are under a court-ordered legal restraint, guardianship, or have been declared legally incompetent.
- **Operational Protocol:**
  - ✓ During onboarding, age verification and self-exclusion database checks are mandatory.
  - ✓ Compliance staff must flag any account where documentation or communication indicates the individual may be under legal restraint or is displaying signs of vulnerability.

- ✓ If a customer is identified as a 'Vulnerable Person,' the account opening process must be terminated immediately. If an existing customer is later identified as vulnerable, the account must be suspended, and any remaining funds handled according to the Responsible Gaming Policy.

## **7. THRESHOLD PROCEDURE XCG 4,000**

- **Detection:** automated cumulative monitoring aggregates deposits, withdrawals and transfers across sessions and payment methods. When cumulative activity  $\geq$  **XCG 4,000**, the threshold process is triggered.
- **Immediate operational controls:** automatic block on deposits and withdrawals; account remains available for gameplay only until CDD is completed.
- **KYC actions:** KYC Team issues a formal document request listing required documents and deadlines; MLRO receives automatic notification and case file is opened in the case management system.
- **Permitted activity during review:** gameplay only; no cash-out or new deposits.
- **Escalation:** if documents indicate high risk or suspicion, escalate to MLRO and Senior Management for decision on restriction, suspension, termination and reporting.

## **8. MISSING DOCUMENTS AT THRESHOLD AND 30-DAY FOLLOW UP**

- **Communication cadence:**
  - ✓ Automated reminder at day 7 and day 21;
  - ✓ Manual outreach by KYC Team at day 14. All outreach attempts are logged in the case file.
- **30-day review:**
  - ✓ If requested information is not received within 30 days of threshold trigger, MLRO reviews the case and recommends one of: extended remediation with documented justification; account suspension pending further action;
  - ✓ Termination of the business relationship. If termination is chosen, the case is documented and reported to the FIU where required.

## **9. ONGOING MONITORING AND RED FLAGS**

- **Monitoring program:**
  - ✓ Automated transaction monitoring rules for velocity, amounts, payment method anomalies, rapid deposit/withdrawal cycles, linked account activity, and cross-jurisdiction transfers.
  - ✓ Alerts are triaged by KYC analysts and escalated to MLRO as needed.

- **Red flags include:**
  - ✓ Sudden change in betting patterns;
  - ✓ Frequent large deposits followed by rapid withdrawals;
  - ✓ Use of multiple payment instruments to circumvent thresholds;
  - ✓ Inconsistent identity information;
  - ✓ Multiple accounts linked to same device or IP;
  - ✓ Customer refusal to provide SoF/SoW when requested.
- **Periodic refresh:**
  - ✓ Risk-based frequency is applied.
  - ✓ Event-driven rescreening occurs on adverse media hits, sanctions list updates, or regulatory alerts.

## **10. POLITICALLY EXPOSED PERSONS SCREENING AND ENHANCED DUE DILIGENCE**

- **Screening frequency:**
  - ✓ At onboarding and continuous automated rescreening (daily).
  - ✓ Event-driven rescreening on adverse media or list updates.
- **PEP handling:**
  - ✓ If a customer or beneficial owner is identified as a PEP, require a signed PEP Declaration Form obtain senior management approval to onboard or continue the relationship, and collect robust SoF/SoW evidence.
  - ✓ Apply enhanced monitoring and shorter refresh intervals.
- **Senior management approval:**
  - ✓ Documented approval required before account activation or continuation for PEPs. Approval must include rationale and mitigation measures.

## **11. SANCTIONS SCREENING, FREEZING AND REPORTING**

- **Lists screened:**
  - ✓ UN, EU, OFAC (US), Curaçao national lists, and relevant local lists in jurisdictions where customers are located.
  - ✓ Screening is automated at onboarding and performed daily or on list updates.
- **Confirmed match procedure:**
  - ✓ Immediately freeze funds and block account activity;
  - ✓ Notify MLRO and Senior Management;
  - ✓ Conduct internal verification to rule out false positives; if match confirmed, follow legal obligations to report to FIU and competent Curaçao authorities and implement asset freezing per applicable law.
  - ✓ Document all steps.

- **False positives:**
  - ✓ Documented clearance process with evidence of independent verification and decision record.

## **12. ACCOUNT RESTRICTIONS, SUSPENSION AND TERMINATION**

- **Restriction types:**
  - ✓ Temporary restriction pending CDD;
  - ✓ Partial restriction (no withdrawals);
  - ✓ Full suspension (no access);
  - ✓ Termination (account closed).
- **Decision authority:**
  - ✓ KYC Team may apply temporary restrictions;
  - ✓ MLRO and Senior Management decide on suspension and termination for high-risk or non-cooperative customers.
  - ✓ All decisions are recorded with rationale and supporting evidence.
- **Handling outstanding balances:**
  - ✓ Follow contractual terms and legal advice;
  - ✓ Where funds are frozen due to sanctions or suspicion, follow reporting obligations and legal requirements for disposition.
- **Resolving disputes:**
  - ✓ The Company is committed to resolving player disputes fairly and transparently. In the event that a dispute remains unresolved through our internal complaints and escalation procedure, the player has the right to refer the matter to an independent Alternative Dispute Resolution (ADR) provider.
  - ✓ The Company utilizes CGA-Certified ADR Provider, an entity certified by the Curaçao Gaming Authority. This ADR service is provided to the player entirely free of charge. Players may initiate the ADR process if they have not received a final response within 8 weeks of their initial complaint or if a 'deadlock' position has been reached. The findings of the ADR provider shall be handled in accordance with the requirements set forth in the LOK and CGA reporting guidelines.

## **13. RECORDKEEPING AND RETENTION**

- **Retention period:**
  - ✓ Retain CDD records, screening results, transaction logs, escalation records, and reporting records for at least five years after the end of the business relationship.
- **Storage and access:**
  - ✓ Records stored securely with access controls;

- ✓ Audit trail for access and changes. Ensure records are retrievable for regulatory requests and audits.

#### **14. TRAINING, AUDIT AND REVIEW**

- **Training:**
  - ✓ Mandatory AML/KYC training for all staff on hire and annually thereafter;
  - ✓ Role-specific training for KYC, payments, and compliance teams.
  - ✓ Training records retained.
- **Audit and testing:**
  - ✓ Internal audit and independent external reviews at least annually;
  - ✓ Remediation plans tracked to completion.
  - ✓ Policy reviewed annually or when regulatory change occurs.

#### **15. ANNEXES AND TEMPLATES**

All annexes below are included verbatim and are ready for operational use. Each annex is a fillable template for case management and regulatory reporting.

##### **ANNEX 1: Onboarding Checklist (fillable template)**

**Purpose:** ensure consistent capture of minimum data and verification steps.

##### **Onboarding Checklist fields (fillable):**

- **Customer ID:** [Customer full name: \_\_\_\_\_]
- **Date of birth:** [DOB: \_\_ / \_\_ / \_\_\_\_]
- **Place of birth:** [Place of birth: \_\_\_\_\_]
- **Nationality:** [Nationality: \_\_\_\_\_]
- **Contact email:** [Email: \_\_\_\_\_]
- **Contact phone:** [Phone: \_\_\_\_\_]
- **Permanent residential address:** [Address: \_\_\_\_\_]
- **Account ID:** [Account ID: \_\_\_\_\_]
- **Identity documents provided:** [Document type: \_\_\_\_\_] [Document number: \_\_\_\_\_] [Expiry date: \_\_ / \_\_ / \_\_\_\_]
- **Proof of address provided:** [Type: \_\_\_\_\_] [Date: \_\_ / \_\_ / \_\_\_\_]

- **Payment method evidence:** [Type: \_\_\_\_\_] [Details: \_\_\_\_\_]
- **Sanctions screening:** [Lists screened: \_\_\_\_\_] [Result: \_\_\_\_\_] [Date/time: \_\_ / \_\_ / \_\_\_\_]
- **PEP screening:** [PEP status: Yes / No] [Source list: \_\_\_\_\_] [Date/time: \_\_ / \_\_ / \_\_\_\_]
- **Vulnerability Check:** [Yes / No] Verified against self-exclusion lists and age requirements no indicators of legal restraint or problem gambling identified
- **Initial risk score:** [Low / Medium / High] [Rationale: \_\_\_\_\_]
- **Verifier name:** [Verifier: \_\_\_\_\_]
- **Verification date:** [Date: \_\_ / \_\_ / \_\_\_\_]
- **Notes:** [Free text: \_\_\_\_\_]
- **Case ID:** [Case ID: \_\_\_\_\_]

**Instructions:** KYC Analyst completes checklist and uploads all documents to the case file. Verification must be completed before enabling withdrawals if threshold rules apply.

**Identification of Vulnerable Persons:** As part of the Customer Due Diligence (CDD) process and in accordance with the National Ordinance on Games of Chance (LOK), Azra 678 performs specific checks to identify 'Vulnerable Persons.' A person is considered vulnerable if they fall into any of the following categories:

- a) Minors: Any individual under the age of 18.
- b) Gambling Addiction: Individuals who have declared a gambling addiction, those currently registered on a self-exclusion list, or those identified through behavioral monitoring as showing signs of problem gambling.
- c) Legal Restraint: Individuals who are under a court-ordered legal restraint, guardianship, or have been declared legally incompetent.

## **ANNEX 2: XCG 4,000 Operational Flowchart**

**Trigger detection:** cumulative deposits/withdrawals/transfers  $\geq$  XCG 4,000.

**Immediate system actions:**

- [ ] Block deposits and withdrawals.
- [ ] Allow gameplay only.
- [ ] Auto-create case file and notify MLRO.

**KYC Team actions checklist (fillable):**

1. ☐ Send formal document request listing required documents and upload instructions.
2. ☐ Log request and set reminders at day 7 and day 21.
3. ☐ Manual outreach at day 14.
4. ☐ Verify documents upon receipt; update risk score.
5. ☐ If verified and risk acceptable, lift deposit/withdrawal block and document decision.
6. ☐ If unresolved at day 30, escalate to MLRO for termination recommendation and FIU reporting.

**Case file reference:** [Case ID: \_\_\_\_\_] **MLRO notified:** [Date/time: \_\_ / \_\_ / \_\_\_\_] [Method: email / system alert]

**ANNEX 3: PEP Declaration Form (fillable template)****PEP Declaration Form**

- **Customer name:** [\_\_\_\_\_]
- **Account ID:** [\_\_\_\_\_]
- **Date:** [\_\_ / \_\_ / \_\_\_\_]
- **Declaration:** I confirm that I am / I am not a Politically Exposed Person. (Tick one) ☐ I am a PEP ☐ I am not a PEP
- **If yes, provide:** Position: [\_\_\_\_\_] Country: [\_\_\_\_\_]  
Office held: [\_\_\_\_\_] Dates in office: [\_\_\_\_\_]  
Relationship to public office: [\_\_\_\_\_]
- **Source of Funds and Source of Wealth provided:** [List documents attached: \_\_\_\_\_]
- **Customer signature:** [\_\_\_\_\_]
- **Verifier name and date:** [\_\_\_\_\_] [\_\_ / \_\_ / \_\_\_\_]
- **Senior Management approval:** Name: [\_\_\_\_\_] Date: [\_\_ / \_\_ / \_\_\_\_]  
Mitigation measures: [\_\_\_\_\_]

**Instructions:** PEPs require senior management approval and enhanced monitoring. Store signed form in case file.

**Note: Definition of Politically Exposed Persons (PEP)**

**1. Prominent Public Functions:**

*A PEP is defined as any individual who is, or has been, entrusted with a prominent public function (foreign domestic or international organization). This includes, but is not limited to:*

*Government & Legislative: Heads of State, Heads of Government, Ministers, State Secretaries, and Members of Parliament.*

*Judicial & Military: Members of supreme courts or high-level judicial bodies, Ambassadors, and high-ranking officers in the armed forces.*

*State-Owned Entities: Senior executives, directors, or members of the board of state-owned enterprises.*

*International Organizations: Directors, deputy directors, and board members of international organizations (e.g., UN, IMF, World Bank).*

*Political Parties: Important officials of political parties.*

*(Note: This does not include middle-ranking or junior officials.)*

**2. Family Members:**

*The status of PEP also extends to immediate family members, which includes:*

*A spouse or a partner considered to be equivalent to a spouse.*

*Children and their spouses or partners.*

*The parents of the person holding the prominent public function.*

**3. Close Associates:**

*A Close Associate includes any individual who is known to have:*

*Joint beneficial ownership of legal entities or legal arrangements with a PEP.*

*Any other close business relationship with a PEP.*

*Sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a PEP.*

#### **4. Duration of Status:**

*In accordance with a risk-based approach, an individual may continue to be treated as a PEP even after they have ceased to hold a prominent public function. The duration of this status is determined by the ongoing risk associated with the individual's influence and the specific nature of the previously held position.*

#### **ANNEX 4: Source of Funds and Source of Wealth Evidence Template (fillable)**

**Acceptable SoF documents:** recent bank statements (3 months); payslips (3 months); sale agreements; inheritance documentation; audited company statements.

**Acceptable SoW documents:** tax returns; employment contract; company ownership documents; property sale deeds.

#### **SoF / SoW Evidence form (fillable):**

- **Customer name:** [\_\_\_\_\_]
- **Account ID:** [\_\_\_\_\_]
- **Document type:** [Bank statement / Payslip / Sale agreement / Other: \_\_\_\_\_]
- **Document date range:** [From \_\_\_\_ / \_\_\_\_ / \_\_\_\_ to \_\_\_\_ / \_\_\_\_ / \_\_\_\_]
- **Document reference:** [\_\_\_\_\_]
- **Verification method:** [Original / Certified copy / Electronic verification]
- **Verifier name:** [\_\_\_\_\_]
- **Verification date:** [\_\_\_\_ / \_\_\_\_ / \_\_\_\_]
- **Notes / corroboration sources:** [\_\_\_\_\_]

**Verification steps:** request originals or certified copies for high risk; corroborate with independent sources; record verification method and verifier.

#### **ANNEX 5: 30-day Reminder and Termination Email Templates (fillable)**

**Day 7 Reminder** Subject: Request for documents to complete your account verification Body: Dear [Customer name: \_\_\_\_\_], We requested documents to verify your account on [date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_]. Please upload the requested documents within 23 days to avoid restrictions. Required documents: [list: \_\_\_\_\_]. If you need assistance, reply to this message. Regards, KYC Team

**Day 21 Final Reminder** Subject: Final reminder to submit KYC documents Body: Dear [Customer name: \_\_\_\_\_], This is a final reminder. If we do not receive the requested documents within 9 days, your account will be reviewed and may be suspended or closed. Required documents: [list: \_\_\_\_\_]. Regards, KYC Team

**Termination Notice** Subject: Account closure due to incomplete verification Body: Dear [Customer name: \_\_\_\_\_], We have not received the requested documents within 30 days. Your account [ID: \_\_\_\_\_] has been closed. If you believe this is an error, contact us with supporting documents. Funds handling: [explain per contract/legal: \_\_\_\_\_]. Regards, MLRO.

#### **ANNEX 6: Escalation Matrix and Service Level Agreements (fillable)**

The Company is committed to resolving player disputes fairly and transparently. In the event that a dispute remains unresolved through our internal complaints and escalation procedure, the player has the right to refer the matter to an independent Alternative Dispute Resolution (ADR) provider.

The Company utilizes CGA-Certified ADR Provider, an entity certified by the Curaçao Gaming Authority. This ADR service is provided to the player entirely free of charge. Players may initiate the ADR process if they have not received a final response within 8 weeks of their initial complaint or if a 'deadlock' position has been reached. The findings of the ADR provider shall be handled in accordance with the requirements set forth in the LOK and CGA reporting guidelines.

#### **Service Level Agreements (SLAs):**

- **KYC Analyst:** first response to alerts within 24 hours.
- **KYC Team Lead:** review within 48 hours for medium risk.
- **MLRO:** review within 72 hours for high risk or sanctions/PEP matches.
- **Senior Management:** decision within 5 business days for termination or complex PEP cases.

#### **Escalation contacts (replace placeholders):**

- **KYC Team Lead:** [Name: \_\_\_\_\_] [Email: \_\_\_\_\_]  
[Phone: \_\_\_\_\_]
- **MLRO:** [Name: \_\_\_\_\_] [Email: \_\_\_\_\_] [Phone: \_\_\_\_\_]
- **Head of Operations:** [Name: \_\_\_\_\_] [Email: \_\_\_\_\_]  
[Phone: \_\_\_\_\_]

- **Legal Counsel:** [Name: \_\_\_\_\_] [Email: \_\_\_\_\_]  
[Phone: \_\_\_\_\_]

**Instructions:** Populate with real contact details and ensure distribution to relevant teams.

## **ANNEX 7: Suspicious Activity Report (SAR) Internal Template and FIU Submission Checklist (fillable)**

### **Internal SAR template fields (fillable):**

- **Customer details:** [Name: \_\_\_\_\_] [Account ID: \_\_\_\_\_]
- **Transaction details:** [Date(s): \_\_ / \_\_ / \_\_\_\_] [Amount(s): \_\_\_\_\_]  
[Payment method(s): \_\_\_\_\_]
- **Reason for suspicion:** [Detailed narrative: \_\_\_\_\_]
- **Supporting documents:** [List and attach: \_\_\_\_\_]
- **Timeline of events:** [\_\_\_\_\_]
- **Actions taken:** [\_\_\_\_\_]
- **MLRO sign-off:** [Name: \_\_\_\_\_] [Date: \_\_ / \_\_ / \_\_\_\_]

### **FIU submission checklist (fillable):**

- ☐ Internal SAR completed and signed by MLRO.
- ☐ All supporting documents attached.
- ☐ Transaction history exported and attached.
- ☐ Evidence of outreach and responses.
- ☐ Legal counsel consulted if required.
- ☐ Date/time of submission to FIU recorded: [\_\_ / \_\_ / \_\_\_\_] [Time: :]

## **ANNEX 8: Sample KYC Case File Log Template (fillable)**

### **KYC Case File Log fields:**

- **Case ID:** [\_\_\_\_\_]

- **Customer ID:** [\_\_\_\_\_]
- **Trigger reason:** [Threshold / Alert / Manual review / Other: \_\_\_\_\_]
- **Documents requested:** [\_\_\_\_\_]
- **Documents received:** [\_\_\_\_\_]
- **Verification outcome:** [Verified / Not verified / Partial]
- **Risk rating:** [Low / Medium / High]
- **Actions taken:** [\_\_\_\_\_]
- **Dates:** [Opened: \_\_ / \_\_ / \_\_\_\_] [Closed: \_\_ / \_\_ / \_\_\_\_]
- **Responsible staff:** [\_\_\_\_\_]
- **Notes:** [\_\_\_\_\_]

**Instructions:** Each KYC case must have a single case file log updated at each step and retained per recordkeeping rules.

#### **ANNEX 9: Device IP and Linkage Investigation Checklist (fillable)**

**Fields to collect:**

- **IP addresses:** [\_\_\_\_\_]
- **Device IDs:** [\_\_\_\_\_]
- **Geolocation anomalies:** [\_\_\_\_\_]
- **Account linkage indicators:** [Shared payment instruments / Shared device / Shared IP / Other: \_\_\_\_\_]
- **Screenshots and logs:** [Attach files: \_\_\_\_\_]
- **Analyst notes:** [\_\_\_\_\_]
- **Escalation required:** [Yes / No] [If yes, escalate to: \_\_\_\_\_]

**Procedure:** run device linkage checks on any suspicious account clusters; document findings and escalate if multiple accounts show linkage to suspicious activity.

#### **ANNEX 10: Policy Change Log (fillable)**

**Policy Change Log table (fillable):**

| Version | Effective date   | Summary of changes                                                                 | Author                  | Approved by             | Review date      |
|---------|------------------|------------------------------------------------------------------------------------|-------------------------|-------------------------|------------------|
| 1.0     | 2026-04-15       | Initial KYC Policy aligned with AML Policy and Allyant guidance; annexes included. | [Name: _____<br>_____]  | [Name: _____<br>_____]  | [____/____/____] |
| [ ]     | [____/____/____] | [_____] [_____] [_____]                                                            | [_____] [_____] [_____] | [_____] [_____] [_____] | [____/____/____] |