

# **Customer Acceptance Policy**

Zoomba B.V.

Next Review: September 2026

## **1. INTRODUCTION**

Zoomba B.V. (“We”, “the Company”, “our”) is registered at 10, Schottegatweg Oost, Unit 1-9, Bon Bini Business Center, Willemstad Curacao. We’ve implemented a comprehensive Customer Acceptance Policy to proactively combat money laundering, terrorism financing, and proliferation risks. Aligned with both local and global regulatory standards, this policy ensures full legal compliance and provides a strong framework for managing risks across all client relationships.

This policy is in strict adherence to the key objectives of Curaçao’s AML/CTF/CPF legislative framework. This includes compliance with the National Ordinance for Games of Chance (LOK), the Criminal Code of Curaçao, the National Ordinance on Offshore Games of Hazard (NOOGH), the National Ordinance Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and the National Ordinance on Identification when Rendering Services (NOIS), with all amendments effective as of May 16, 2024. Additionally, it adheres to the Sanctions National Ordinance (SNO) and the Kingdom Sanction Act.

Beyond national regulations, the Company’s policy incorporates leading international standards and guidelines, including the Financial Action Task Force (FATF) Recommendations, the European Union’s Anti-Money Laundering Directives (4th, 5th, and 6th AMLDs), and the Wolfsberg Principles.

The Customer Acceptance Policy applies to all directors, officers, employees, contractors, and any third parties involved in onboarding or verification activities for Zoomba B.V. Customers will only be granted access to deposit, withdraw, or place wagers once they have successfully met the acceptance criteria outlined in this policy and completed all mandatory verification and screening procedures.

## **2. APPLICABILITY**

This policy applies to all individuals seeking to open an account with Zoomba B.V., regardless of the registration channel. This includes account creation via the company’s official website, mobile applications, third-party platforms, and affiliate partnerships.

The policy governs the customer relationship from the initial application stage through to account closure or termination.

## **CUSTOMER ONBOARDING REQUIREMENTS**

Zoomba B.V. accepts only customers who fully meet all applicable legal, regulatory, and internal compliance standards. The minimum acceptance criteria include verification that the customer has reached the legal gambling age, which is at least eighteen years or higher if required by the laws of the customer's jurisdiction of residence. All applicants must provide accurate and verifiable details, including full legal name, date and place of birth, nationality, and current residential address.

Zoomba B.V. does not accept customers who are residents of, located in, or transacting from jurisdictions prohibited under Curaçao's regulatory framework, international sanctions regimes, or the company's own restricted jurisdictions list. All applicants are screened against sanctions lists issued by the United Nations, the European Union, the United States Office of Foreign Assets Control, the United Kingdom Office of Financial Sanctions Implementation, the Sanctions National Ordinance, the Kingdom Sanction Act, and any relevant lists maintained by the Curaçao Gaming Control Board.

The company requires that all funds used for gambling activities originate from legitimate and lawful sources. Where risk assessment deems it necessary, customers must provide documentary evidence of the source of funds and, if applicable, the source of wealth. Individuals or entities with a known history of fraud, self-exclusion for problem gambling, chargebacks, bonus abuse, or violations of gambling regulations will be denied access to services.

### **3. RISK-BASED CUSTOMER ASSESSMENT**

Zoomba B.V. applies a comprehensive risk-based approach to the acceptance and ongoing assessment of its customers. This method ensures that the level of due diligence applied is proportionate to each customer's risk profile and is determined by multiple factors, including customer-specific, product-related, geographic, and technological risks.

#### **3.1 Customer Risk Profiling**

Every prospective customer undergoes a structured assessment to determine their potential exposure to risks such as money laundering, terrorist financing, and proliferation financing. The risk profile assigned to a customer dictates the level of due diligence required and the intensity of ongoing monitoring.

Customers assessed as low risk generally demonstrate a stable financial background, a clear and well-documented source of income, employment in sectors considered low-risk from an AML perspective, and betting behaviour that is consistent with their stated financial means.

By contrast, high-risk customers may present with multiple or non-transparent income sources, occupations in industries with heightened AML exposure (e.g., cryptocurrency trading platforms, unregulated financial services), or gambling activity that deviates significantly from their disclosed financial profile. Politically Exposed Persons (PEPs), as well as their relatives and close associates, are automatically categorized as high risk and subject to enhanced controls.

Zoomba B.V. evaluates each customer across a range of indicators, many of which may trigger classification as higher risk. Customers falling into any of the following categories are subject to Enhanced Due Diligence (EDD) procedures, which include more detailed verification, source of wealth assessments, ongoing monitoring, and in some cases, senior management approval before continued account activity.

- **Multiple income sources**

Customers with more than one source of income must provide evidence for each declared stream, such as payslips, audited business accounts, tax filings, or investment statements. Verification must confirm both legitimacy and lawfulness.

- **Irregular or unstable income**

Where income is seasonal, commission-based, or inconsistent, customers must demonstrate with supporting documentation that gambling funds are derived from legitimate sources. Additional monitoring is implemented to identify anomalies.

- **Politically Exposed Persons (PEPs)**

PEPs, together with their family members and associates, are subject to automatic high-risk classification. Enhanced Due Diligence includes verifying source of funds and wealth, conducting ongoing transaction reviews, and requiring senior management sign-off prior to account approval.

- **High-value or frequent spenders**

Customers wagering unusually large sums or engaging in high-frequency

betting must prove that their funds are legitimate. Acceptable documentation may include bank statements, tax records, or verified income evidence.

- **Spending inconsistent with declared income**

If a customer's gambling activity exceeds what can reasonably be supported by their known income or assets, further investigation is required. Customers must provide additional verification to justify the discrepancy.

- **Casual or local customers with sudden behavioural changes**

Significant, unexplained increases in gambling by individuals previously assessed as low-risk trigger a reassessment and may result in reclassification to higher risk.

- **Improper third-party involvement**

Evidence that a customer is using third parties to place bets, transfer funds, or cash out winnings is immediately escalated. Both the customer and the third party are subject to full verification, and all related transactions are investigated for suspicious activity.

- **Multiple or duplicate accounts**

Customers attempting to maintain more than one account to obscure gambling activity or avoid monitoring are identified through internal systems. All related accounts are consolidated and subject to review.

- **Unidentified customers redeeming large chip values**

Situations where a customer with no established gambling history attempts to redeem substantial amounts of chips are suspended until identity, source of funds, and source of chips are verified.

- **Junket-related activity**

Customers associated with junket operators are automatically considered high risk. In such cases, EDD extends to both the customer and the junket operator, requiring verification of all financial arrangements, credit extensions, and funding sources.

This structured profiling process ensures that Zoomba B.V. can apply proportionate controls, maintain compliance with regulatory obligations, and mitigate exposure to financial crime risks.

### **3.2 Risks Related to Products, Services, and Transactions**

The overall risk level also depends on the type of products and services a customer engages with. Certain offerings, such as peer-to-peer transfers, the purchase or exchange of gaming tokens, or payment channels that allow anonymous or semi-anonymous funding (e.g., prepaid cards or some cryptocurrencies), carry elevated risks due to their reduced traceability.

Accounts primarily used for financial movement rather than genuine gaming activity — for example, those with large deposits followed by minimal play and quick withdrawals — are subject to enhanced scrutiny. Likewise, the use of payment instruments not registered in the name of the account holder is flagged as suspicious and requires further verification.

Zoomba B.V. monitors the following transaction and product-related risk factors closely. Where identified, proportionate mitigating measures and, if necessary, escalation procedures are applied:

- **Proceeds of crime**

Funds suspected of originating from illicit activity (e.g., cheque fraud, card fraud, narcotics trafficking, or workplace theft) must be verified for lawful origin. Any suspected criminal proceeds are reported to the Financial Intelligence Unit (FIU).

- **Anonymous payment methods**

The use of prepaid cards, virtual assets, or other anonymous instruments is treated as high risk. Customers must undergo strict verification, with funds traced back to legitimate sources.

- **Improper use of casino accounts**

Accounts are to be used exclusively for gambling purposes. Deposit–withdrawal behaviour without genuine play triggers immediate review and possible suspension.

- **Third-party accounts or cards**

When customer accounts are funded by payment methods not in the customer's name, both parties must be fully verified, and their relationship established.

- **Transfers between gaming accounts**

Transfers are generally prohibited unless backed by legitimate business reasons. All such transactions require Compliance Officer approval and full

documentation.

- **Multiple accounts or wallets**

Use of multiple accounts to obscure gambling activity or bypass controls is detected by internal monitoring. All linked accounts are reviewed collectively.

- **Frequent changes to funding methods**

Repeatedly switching bank accounts or payment methods raises red flags. Such customers are re-profiled and may be subjected to Enhanced Due Diligence.

- **Identity fraud**

Use of stolen identities or account details to fund gambling accounts is countered with document authentication and verification checks. All suspected cases are reported per regulatory requirements.

- **Electronic wallets**

E-wallets not licensed in reputable jurisdictions present heightened AML risk, particularly when they allow anonymous cash deposits. Customers must prove the source of funds, and providers must be confirmed as operating under adequate AML/CFT regulations

### **3.3 Jurisdictional and Geographic Risk Assessment**

Zoomba B.V. operates a dynamic geographic risk classification framework to evaluate both the customer's country of residence and the origin of their funds. This framework is informed by internationally recognized sources, including Financial Action Task Force (FATF) public statements, Caribbean Financial Action Task Force (CFATF) advisories, the European Commission's list of high-risk third countries, the U.S. Office of Foreign Assets Control (OFAC) sanctions lists, the U.S. Department of State's International Narcotics Control Strategy Reports, and Transparency International's Corruption Perceptions Index (CPI).

Customers originating from high-risk jurisdictions are only onboarded following the application of Enhanced Due Diligence (EDD), while customers from sanctioned jurisdictions are categorically rejected.

Zoomba B.V. considers a jurisdiction high risk if it demonstrates one or more of the following characteristics:

- **Weak AML/CFT frameworks**

Countries without robust anti-money laundering or counter-terrorist

financing laws, regulations, or enforcement mechanisms are deemed high risk. Customers must provide comprehensive documentation covering their source of funds and source of wealth, and their activity is subject to close and ongoing monitoring.

- **Systemic corruption**

Jurisdictions where corruption is widespread are treated as elevated risk. Customers from these countries undergo stricter verification, particularly regarding the legitimacy of income.

- **Sanctioned jurisdictions**

Countries under international sanctions for terrorism, proliferation of weapons of mass destruction, or related activities are not accepted. Any exceptional cases would require explicit senior management approval, accompanied by exhaustive EDD.

- **Terrorist activity**

Jurisdictions with known terrorist organizations operating within their borders are classified as high risk. Customers from these locations require enhanced verification, continuous transaction monitoring, and periodic reviews.

To determine geographic risk, Zoomba B.V. references the following authoritative lists and statements:

- FATF list of High-Risk Jurisdictions subject to a Call for Action
- FATF list of Jurisdictions under Increased Monitoring
- CFATF Public Statements and advisories
- European Commission list of third countries with strategic AML/CFT deficiencies
- U.S. Department of State International Narcotics Control Strategy Report (jurisdictions of concern/primary concern)
- OFAC sanctions lists
- Transparency International Corruption Perceptions Index

- Credible reports identifying jurisdictions supporting or hosting terrorist organizations

If a customer's country of residence or source of funds appears on any of these lists, the case is escalated to the Compliance Officer for a full review. Onboarding may proceed only after EDD measures are completed, which include verifying identity, source of funds, and source of wealth, along with enhanced transaction monitoring throughout the customer relationship.

### **3.4 Access Channel and Technology Risks**

The level of customer risk is also influenced by the channels through which they interact with the company. Remote onboarding without face-to-face verification heightens the possibility of identity fraud or impersonation. Zoomba B.V. mitigates this risk through robust digital Know Your Customer processes, including biometric verification, document authenticity checks, geolocation validation, and multi-factor authentication.

All new technological developments, payment methods, or platform features undergo a pre-launch risk assessment to ensure they cannot be exploited for illicit purposes.

Zoomba B.V. monitors the following access channel risks closely:

- **Channels that favour anonymity**  
Any method that allows customers to remain anonymous poses an elevated risk. Registration or funding through such channels is only permitted after strict verification, including biometric checks, document validation, and real-time screening against sanctions and PEP lists.
- **Non-face-to-face interaction**  
While remote onboarding and transactions are standard, they still carry inherent risk. The company mitigates this with secure technologies such as liveness detection, biometric verification, and document authenticity checks to prevent impersonation or fraud.
- **Third-party involvement**  
When third parties facilitate a customer's interaction with Zoomba B.V. , the risk increases — especially if the intermediary is not subject to AML/CFT obligations. In such cases, due diligence is applied to both the customer and the intermediary, including verification of regulatory status,

AML/CFT controls, and the accuracy of provided information.

### **3.5 Risk Assessment Indicators**

Zoomba B.V. identifies and evaluates risk indicators across several categories to ensure a structured and proportionate risk-based approach (RBA) to customer due diligence. These indicators highlight potential vulnerabilities linked to customer behaviour, product usage, geographic exposure, and distribution channels.

#### **Key Categories of Risk Indicators:**

- **Customer Risk Profile:** Examples include multiple or unclear income sources, irregular income streams, Politically Exposed Persons (PEPs), high or disproportionate spenders, casual customers with sudden shifts in spending, improper third-party involvement, multiple or duplicate accounts, unknown customers redeeming large chip amounts, or links to junket operations.
- **Product, Service, and Transaction Risks:** Risks such as funds linked to criminal activity, large or suspicious cash transactions, anonymous or semi-anonymous funding methods (e.g., prepaid cards, cryptocurrency), misuse of accounts for non-gaming financial flows, third-party funding, account-to-account transfers, use of multiple wallets, frequent changes of payment methods, identity fraud, and high-risk e-wallet providers.
- **Geographic Risks:** Customers from jurisdictions with weak AML/CFT frameworks, high levels of corruption, countries subject to sanctions, or those with terrorism financing concerns. Jurisdictions listed by FATF, CFATF, OFAC, the European Commission, or Transparency International's Corruption Perceptions Index are closely monitored.
- **Access Channel Risks:** Anonymity-favouring channels, remote onboarding without adequate technology safeguards, and unregulated or high-risk third-party involvement.

Zoomba B.V. applies a structured Risk Calculator to assess each customer relationship. Every factor is assigned a weighted score, which determines whether the customer falls into low, medium, or high-risk categories.

#### **Risk Classification Framework:**

- **Low Risk** – Standard Customer Due Diligence (CDD) applies. Documentation is collected only if legally required or if the risk profile changes.
- **Medium Risk** – Standard CDD supplemented by additional verification checks, with closer monitoring of activity.
- **High Risk** – Enhanced Due Diligence (EDD) is mandatory. This includes senior management approval prior to onboarding, full source of wealth verification, and continuous enhanced monitoring.

#### **Illustrative Risk Indicators by Category:**

- **Purpose of Account Registration**
  - Low: Recreational gambling, casual entertainment.
  - Medium: Semi-professional or professional gambling activity.
  - High: Bonus abuse, arbitrage play, or financially exploitative activity.
- **Source of Funds**
  - Low: Salary, pension, or low-risk investments.
  - Medium: Business income, legitimate winnings, inheritance, asset sales, gifts/loans.
  - High: Cryptocurrency without transparent history, unverifiable offshore sources.
- **Source of Wealth**
  - Low: Long-term employment income, stable business ownership, inheritance from close relatives, long-term investment growth.
  - Medium: Property or business sales, lottery or gambling winnings.
  - High: High-risk or speculative investments (crypto, forex), offshore accounts, unverifiable wealth claims.
- **Transaction Frequency**

- Low: Monthly.
- Medium: Weekly.
- High: Daily or near-daily.

- **Transaction Value (NAF)**

- Low: Up to 1,000.
- Medium: 1,000 – 4,000.
- High: Above 4,000.

- **Incoming Payments**

- Low: Bank transfers, debit/credit cards.
- Medium: E-wallets, prepaid cards.
- High: Cryptocurrency deposits, third-party payments, deposits from high-risk jurisdictions, unregulated processors, unusual or high-value patterns.

- **Outgoing Payments**

- Low: Standard withdrawals or refunds.
- Medium: Bonus cash-outs, frequent or large withdrawals.
- High: Third-party withdrawals, crypto withdrawals, chargebacks, linked accounts, suspicious withdrawal activity.

- **Gaming Behaviour**

- Low: Casual, consistent, moderate betting.
- Medium: Long sessions, high-frequency betting, significant variation in stakes.
- High: Rapid stake escalation, chasing losses, collusion, multi-accounting, or other suspicious/fraudulent patterns.

- **Payment Channels**

- Low: Bank transfers.
- Medium: Licensed e-wallets.
- High: Cryptocurrencies, prepaid cards, or other anonymous methods.

- **Adverse Media**

- Low: No negative records.
- Medium: Unverified allegations or speculative reports.
- High: Verified links to crime, financial misconduct, or other illicit activity.

The final composite score produced by the Risk Calculator determines the level of due diligence applied to the customer. This ensures that resources are directed proportionately, with high-risk customers subject to stringent monitoring and oversight in line with Zoomba B.V. 's AML/CFT obligations.

## **5 COMPLIANCE WITH LEGISLATIVE FRAMEWORK**

Zoomba B.V. acknowledges that the Customer Acceptance Policy is a core element of its broader Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) framework. The company is committed to operating in strict accordance with Curaçao's legal and regulatory obligations, including the National Ordinance on Identification when Rendering Services, the National Ordinance on the Reporting of Unusual Transactions, the Sanctions National Ordinance, the Kingdom Sanction Act, and the National Ordinance on Games of Chance.

Compliance with these requirements is regarded as a fundamental operational priority. Customer acceptance measures are fully embedded into Zoomba B.V. 's compliance systems, ensuring that due diligence is not confined to onboarding but is maintained across the entire customer lifecycle. Any significant change in a customer's risk profile, transactional activity, or jurisdiction is promptly identified and addressed.

All personnel involved in onboarding and verification processes are required to undergo dedicated training on Curaçao's legislative framework and the company's internal compliance standards. This training covers the practical application of the risk-based approach, identification of high-risk indicators, and the correct procedures for escalation to senior management or the Compliance Officer.

To ensure the robustness of its program, Zoomba B.V. engages independent auditors at least once per year to assess the effectiveness of its risk-based approach within the Customer Acceptance Policy. These reviews evaluate identity verification procedures, sanctions screening, the application of Enhanced Due Diligence (EDD), and ongoing monitoring of customers. Audit findings are formally reported to the Board of Directors, and any gaps or weaknesses are promptly remediated through corrective actions within defined timelines.

## **6. CUSTOMER ONBOARDING PROCESS**

The onboarding of customers at Zoomba B.V. is carried out through a structured and fully documented process, ensuring that only applicants who satisfy the company's acceptance criteria are granted access to its services. No account is activated until all stages of identification, verification, and sanctions screening have been successfully completed.

As part of onboarding, Zoomba B.V. collects key personal information, including the customer's full legal name, date and place of birth, nationality, residential address, and an official identification number. Each applicant is screened against sanctions and Politically Exposed Person (PEP) lists prior to approval. This screening is performed using automated tools for broad coverage, with alerts or potential matches reviewed manually by trained compliance staff to ensure accuracy and eliminate false positives.

For customers identified as high risk through the initial assessment, additional documentation is required to confirm both the legitimacy of their funds and, where relevant, their source of wealth. Acceptable evidence may include bank statements reflecting regular income deposits, audited business accounts, tax filings, property sale contracts, or investment portfolio statements.

## **7. ONGOING MONITORING**

Zoomba B.V. recognises that customer acceptance is not limited to the onboarding stage. Continuous monitoring is essential to ensure that customer activity remains aligned with the profile established at the time of registration.

The company operates automated transaction monitoring systems designed to flag unusual or suspicious behaviour. Such behaviour may include deposits or withdrawals that do not match the customer's known profile, rapid fund movement without meaningful gameplay, the use of multiple or unusual payment methods, or activity patterns that suggest collusion, chip-dumping, or other prohibited practices. All system-generated alerts are reviewed promptly by compliance officers, who determine whether escalation or further investigation is required.

Beyond real-time monitoring, Zoomba B.V. carries out scheduled reviews of customer profiles, applying a risk-based approach to determine frequency and scope. Dynamic re-assessments are also conducted when significant changes occur, such as relocation to a high-risk jurisdiction, a sharp increase in transaction activity, or other material developments that may alter the customer's risk rating.

## **8. ENHANCED DUE DILIGENCE**

Enhanced Due Diligence, referred to as EDD, is applied to customers who present an elevated risk profile. This includes politically exposed persons, customers from jurisdictions classified as high risk, customers engaging in unusually large or complex transactions, and customers whose financial activity does not correspond with their stated income or business activities.

EDD measures include the collection of more detailed information and verification to a higher standard than that required for standard due diligence. The process involves thorough analysis of the customer's source of funds and source of wealth, supported by multiple independent and credible sources. This may include corporate registry searches, verification of employment or business ownership, review of audited financial statements, and comprehensive adverse media checks.

Approval of high-risk customers requires sign-off from senior management, and in certain cases, the Compliance Officer may seek formal approval from the Board of Directors. Once onboarded, these customers are subject to heightened monitoring measures, which may include lower transaction thresholds, enhanced transaction scrutiny, and more frequent profile reviews to ensure compliance with this policy.

## **9. TERMINATION OF CUSTOMER RELATIONSHIPS**

Zoomba B.V. reserves the right to end its relationship with any customer who fails to provide the required documentation within thirty (30) calendar days, engages in conduct that raises reasonable suspicion of money laundering, terrorist financing, or proliferation financing, or breaches applicable laws or the company's Responsible Gambling Policy.

Where termination is linked to suspected criminal activity, Zoomba B.V. will submit a report to the Financial Intelligence Unit in line with the National Ordinance on the Reporting of Unusual Transactions. Any balance remaining in the customer's account will be refunded to the original funding source, unless legal requirements mandate that the funds be frozen or seized pending investigation. All account closures are recorded in detail, and relevant records are retained for a minimum of five years.

Zoomba B.V. will decline or discontinue services in any of the following circumstances:

- The customer resides in, is located in, or transacts from a prohibited jurisdiction or a jurisdiction subject to sanctions.
- The customer fails to submit required information or documentation within specified deadlines under CDD or EDD requirements.
- The customer provides false, misleading, or incomplete information during registration or verification.
- The customer's source of funds or wealth cannot be reasonably verified as legitimate.
- The customer is identified as being involved in, or reasonably suspected of, money laundering, terrorist financing, or other forms of criminal activity.
- The customer is a Politically Exposed Person (PEP) whose risk cannot be mitigated to an acceptable level.
- The customer engages in fraudulent activity, bonus abuse, collusion, or other prohibited gambling practices.
- The customer attempts to transact through third parties without full disclosure and verification.
- The customer has previously self-excluded or been excluded by the company under responsible gambling protocols.
- The customer seeks to redeem large sums of chips or winnings without verifiable gambling activity to support the funds.
- The customer is underage or otherwise below the legal gambling age in their jurisdiction.

## **10. INTEGRATION WITH RESPONSIBLE GAMING**

The Customer Acceptance Policy is fully aligned with Zoomba B.V. 's Responsible Gambling Policy, ensuring that customer protection measures are embedded into all stages of the relationship. Where a customer demonstrates signs of gambling-related harm — such as frequent deposits that appear disproportionate to their financial means or excessively long gaming sessions — the company may intervene by applying restrictions, suspending the account, or declining further service.

Requests for self-exclusion are actioned without delay and applied consistently across all accounts connected to the customer, preventing attempts to bypass exclusion measures. Additionally, all staff in customer-facing roles receive targeted training to recognise early indicators of problem gambling, both during the onboarding process and throughout ongoing monitoring.

## **11. RECORD KEEPING**

Zoomba B.V. maintains all documentation related to customer acceptance for a minimum of five years after the business relationship has been terminated. This includes, but is not limited to, identification documents, proof of address, evidence of source of funds and wealth, transaction monitoring records, Enhanced Due Diligence (EDD) files, internal compliance notes, and records of account closures or relationship terminations.

All records are stored in encrypted form with strict access controls. Only authorised personnel may access these records, and every access attempt is logged and subject to periodic review to ensure full compliance with data protection, confidentiality, and regulatory obligations.

## **12. POLICY REVIEW AND APPROVAL**

The Customer Acceptance Policy is reviewed at least once every twelve months to confirm its continued effectiveness and alignment with legislative requirements, regulatory guidance, and recognised best practices. The review process also considers changes in the company's risk profile, evolving customer behaviour patterns, and technological developments that may introduce new risks.

Any proposed amendments are drafted by the Compliance Officer and submitted to the Board of Directors for formal approval prior to implementation. All revisions are fully documented, and affected staff are notified and trained to ensure the updated policy is applied consistently across the organisation.