

Surewin B.V

Operations Manual

Version 1

Company Name: Surewin B.V
Effective Date: 26 June 2026
Document Owner: Craig Murugan
ADR Provider: CADRE

DOCUMENT CONTROL

CONTENTS

VERSION CONTROL	10
1. PURPOSE OF THIS OPERATIONS MANUAL.....	11
1.1 Purpose	11
1.2 Nature of this Manual	11
1.3 Objectives	11
2. SCOPE AND APPLICATION	12
2.1 Scope	12
2.2 Who this manual applies to:	12
2.3 Obligation to Comply	12
3. REGULATORY FRAMEWORK	13
3.1 Regulatory Basis.....	13
3.2 Core Regulatory and Control Objectives	13
3.3 Regulatory Cooperation	13
4. RELATIONSHIP WITH OTHER POLICIES AND PROCEDURES	13
4.1 Related Documents.....	13
4.2 Hierarchy of Documents	14
4.3 Supporting SOPs and Team Procedures	14
5. DEFINITIONS.....	14
6. Licensed activities.....	15
7. GOVERNANCE STRUCTURE AND OVERSIGHT	15
7.1 Governance Principle	15
7.2 Board Responsibility	15
7.3 Senior Management Oversight	15
7.4 Control Functions	16
8. ROLES AND RESPONSIBILITIES.....	16
8.1 Board	16

8.2 Managing Director / Senior Management	16
8.3 Compliance Officer	16
8.4 MLRO	17
8.5 Responsible Gambling Officer.....	17
8.6 Customer Support / Operations Manager.....	17
8.7 Risk / Fraud / Payments Owner.....	17
8.8 Finance / Reconciliation Owner	18
8.9 IT / Security Owner	18
8.10 All Employees.....	18
9. DELEGATED AUTHORITY AND APPROVAL FRAMEWORK	18
9.1 Principle	18
9.2 Matters Requiring Escalated Approval.....	18
9.3 Approval Matrix	19
10. WHISTLEBLOWING AND PROTECTED DISCLOSURES	19
10.1 Principle	19
10.2 No Retaliation	19
10.3 Matters That May Be Reported	19
10.4 Reporting Channels	20
10.5 Confidentiality	20
10.6 Recordkeeping.....	20
11. DOCUMENT GOVERNANCE AND REVIEW CYCLE	20
11.1 Document Ownership	20
11.2 Review Frequency	20
11.3 Version Control	20
11.4 Controlled Copies	21
12. BUSINESS OVERVIEW	21
12.1 Business Model.....	21
12.2 Core Operating Functions	21
12.3 Player Lifecycle Overview	21
12.4 GAMING OPERATIONS, PRODUCTS AND SERVICES	21
12.5 GAMES OF CHANCE, BETTING AND OUTCOME DETERMINATION	23
12.6 PLAYER WEBSITE AND INTERFACE	24
13. ORGANISATIONAL STRUCTURE AND DEPARTMENTS	26
13.1 Organisational Structure.....	26

OPERATIONAL STRUCTURE.....	27
13.2 Departmental Coordination	27
14. CRITICAL SYSTEMS, PLATFORMS AND TOOLS	27
14.1 System Register	27
14.2 Access Principle	28
14.3 System Dependencies.....	28
14.4 TECHNICAL INFRASTRUCTURE OVERVIEW	28
14.5 Technical Infrastructure Diagram.....	29
15. OUTSOURCING AND CRITICAL SUPPLIER OVERSIGHT	29
15.1 Outsourcing Principle.....	29
15.2 Critical Suppliers	30
15.3 Oversight Requirements	30
15.4 OPERATIONAL QUALITY MONITORING AND TESTING.....	30
16. CUSTOMER REGISTRATION AND ACCOUNT OPENING - PLAYER ACCOUNT LIFECYCLE OPERATIONS	31
16.1 Account Registration	31
16.2 Age and Eligibility Gate.....	31
16.3 Initial Screening	32
16.4 Manual Review Triggers at Onboarding	32
17. CUSTOMER DUE DILIGENCE / KYC PROCEDURE	32
17.1 KYC Obligation	32
17.2 Standard KYC Information and Documents	32
17.3 Trigger Events for KYC Review	33
17.4 KYC Workflow.....	33
17.5 Failure to Complete Verification	33
18. ENHANCED DUE DILIGENCE, SOURCE OF FUNDS, SOURCE OF WEALTH AND BENEFICIAL OWNERSHIP	33
18.1 EDD Requirement	33
18.2 EDD Measures	34
18.3 Source of Funds / Source of Wealth Review	34
18.4 Beneficial Ownership / Third-Party Funding Concerns	34
19. PEP, SANCTIONS AND ADVERSE MEDIA SCREENING.....	34
19.1 Screening Requirement.....	34
19.2 Positive Match Handling.....	34

19.3 PEP Customers	35
20. RESTRICTED JURISDICTIONS AND PROHIBITED CUSTOMERS	35
20.1 Restricted Jurisdiction Controls	35
20.2 Detection and Escalation	35
21. ACCOUNT RESTRICTIONS, SUSPENSION, BLOCKING AND CLOSURE	35
21.1 Grounds for Restriction or Suspension	35
21.2 Operational Controls	36
21.3 Account Closure	36
22. DORMANT ACCOUNTS AND REACTIVATION	36
22.1 Dormancy	36
22.2 Reactivation	36
23. DEPOSIT ACCEPTANCE CONTROLS	36
23.1 Purpose	36
23.2 Deposit Acceptance Principle	36
23.3 Payment Method Controls	37
23.4 Deposit Monitoring	37
23.5 Deposit Restrictions	37
23.6 Recordkeeping	37
24. PLAYER FUNDS, WALLETS AND BALANCE CONTROLS	38
24.1 Player Balance Integrity	38
24.2 Wallet and Ledger Controls	38
24.3 Segregation of Duties	38
24.4 Reconciliations and Exception Review	38
25. WITHDRAWAL REVIEW AND APPROVAL PROCEDURE	38
25.1 Withdrawal Review Principle	38
25.2 Standard Withdrawal Review	39
25.3 Withdrawal Hold or Escalation Triggers	39
25.4 Approval and Release	39
25.5 Rejection, Refusal or Confiscation	39
25.6 Withdrawal Recordkeeping	39
26. UNWAGERED DEPOSITS, WITHDRAWAL HOLDS AND SOURCE OF FUNDS REVIEWS	40
26.1 Unwagered or Minimally Used Funds	40
26.2 Source of Funds and Purpose Review	40
26.3 Withdrawal Holds Pending Review	40

27. FRAUD, MULTIPLE ACCOUNTS, CHARGEBACKS AND BONUS ABUSE	41
27.1 Fraud Prevention Objective.....	41
27.2 Fraud Indicators.....	41
27.3 Fraud Review Actions	41
27.4 Chargeback Handling	41
27.5 Confiscation / Forfeiture Decisions	41
28. MANUAL ADJUSTMENTS, DUAL CONTROLS AND RECONCILIATIONS	42
28.1 Manual Adjustment Principle.....	42
28.2 Adjustment Controls.....	42
28.3 Dual Control for Sensitive Actions	42
28.4 Reconciliation and Oversight	42
28.5 Management Review and Escalation.....	42
AML/CFT OPERATIONS	43
29. AML/CFT GOVERNANCE FRAMEWORK	43
29.1 Purpose.....	43
29.2 AML/CFT Objectives.....	43
29.3 AML/CFT Roles and Responsibilities.....	44
(a) First line – Operational and customer-facing staff	44
(b) Second line – Compliance / AML oversight.....	44
(c) Third line / decision authority – MLRO	44
29.4 No Tipping-Off.....	44
30. CUSTOMER RISK ASSESSMENT AND ONGOING MONITORING	45
30.1 Risk-Based Approach.....	45
30.2 Ongoing Monitoring Requirement	45
30.3 Monitoring Sources.....	45
30.4 Internal Risk Categorisation	45
31. EDD / SOF / SOW / PEP / SANCTIONS ESCALATION TRIGGERS	46
31.1 General Principle.....	46
31.2 EDD Triggers	46
31.3 Source of Funds / Source of Wealth Review.....	46
31.4 PEP Escalation.....	47
31.5 Sanctions Escalation	47
32. SUSPICIOUS ACTIVITY INDICATORS	47
32.1 Purpose.....	47

32.2 Suspicious Indicators at Onboarding / Registration Stage	47
Identity / KYC concerns	47
Duplicate / linked account indicators	48
Geography / sanctions / profile concerns	48
Behavioural red flags at registration	48
32.3 Suspicious Indicators During the Active Relationship	48
Transaction behaviour	48
Withdrawal behaviour	48
Customer explanations and conduct	49
32.4 Additional High-Risk Indicators	49
33. LINKED TRANSACTIONS / STRUCTURING / AGGREGATION INDICATORS	49
33.1 Purpose	49
33.2 Linked Transaction Indicators	49
33.3 Structuring / Threshold Avoidance Indicators	49
33.4 Low-Value / High-Volume Patterns	50
33.5 Aggregation Requirement	50
34. INTERNAL UNUSUAL TRANSACTION / SUSPICIOUS ACTIVITY ESCALATION	50
34.1 Obligation to Escalate	50
34.2 When to Escalate	50
34.3 Escalation Recipient	51
34.4 Information Required in an Internal Escalation	51
34.5 Timing and Follow-Up	51
34.6 Customer Communication During Escalation	51
35. INTERNAL INVESTIGATION PROCEDURE	51
35.1 Purpose	51
35.2 Investigation Standard	52
35.3 Investigation Steps	52
35.4 Case Notes	52
35.5 No Tipping-Off During Investigation	52
36. REASONABLE GROUNDS FOR SUSPICION / INTERNAL UTR REPORTING	52
36.1 Escalation Threshold	52
36.2 Internal Reporting Standard	52
Who?	53
What?	53

When?	53
Why?	53
36.3 Reviewer Role vs MLRO Role	53
37. FIU CURAÇÃO goAML REPORTING PROCEDURE.....	53
37.1 Purpose	53
37.2 Reporting Authority	53
37.3 goAML Access and Registration	53
37.4 Submission Procedure	54
37.5 Supporting Evidence	54
37.6 Confidentiality	54
38. MLRO INVESTIGATION REGISTER	54
38.1 Purpose	54
38.2 Minimum Register Fields.....	54
38.3 Registering Non-Reportable Cases	55
38.4 Periodic Review Use	55
39. AML REGISTERS, RECORDKEEPING, TRAINING AND AUDIT	55
39.1 AML Register Suite	55
39.2 Recordkeeping.....	55
39.3 AML Training.....	56
39.4 Audit and Quality Assurance.....	56
40. RESPONSIBLE GAMBLING GOVERNANCE	56
40.1 Purpose	56
40.2 Responsible Gambling Objective	56
40.3 Governance and Ownership	56
40.4 Shared Responsibility Across the Business	57
40.5 Relationship with the Responsible Gambling Policy	57
41. AGE VERIFICATION AND UNDERAGE GAMBLING CONTROLS	57
41.1 No Minor Play	57
41.2 Age Verification Controls	57
41.3 Underage Escalation Procedure	57
41.4 Recordkeeping.....	57
42. VULNERABLE CUSTOMER IDENTIFICATION AND RISK CLASSIFICATION	58
42.1 Purpose	58
42.2 Sources of RG Risk Indicators	58

42.3 Risk-Based RG Classification	58
42.4 Escalation Requirement	58
42.5 Interaction with AML, Fraud and Complaints.....	59
43. RG INTERVENTIONS, CUSTOMER CONTACT AND SAFER GAMBLING ACTIONS	59
43.1 Principle	59
43.2 Types of RG Action.....	59
43.3 Direct Customer Contact.....	59
43.4 Promotional Suppression	59
43.5 Follow-Up and Ongoing Monitoring	60
44. LIMITS, COOLING-OFF, SELF-EXCLUSION AND OPERATOR-IMPOSED RESTRICTIONS	60
44.1 Customer Protection Tools	60
44.2 Cooling-Off Requests.....	60
44.3 Self-Exclusion Requests	60
44.4 Operator-Imposed Restrictions or Exclusions	60
44.5 Reactivation Controls	60
45. RG RECORDS, ESCALATIONS AND REPORTING	61
45.1 RG Records	61
45.2 RG Escalation.....	61
45.3 RG Reporting	61
46. CUSTOMER SUPPORT OPERATING MODELWEBSITE AND PLAYER INTERFACE CONTROLS - COMPLAINTS AND ADR	61
46.1 Support Function	62
46.2 Support Responsibilities.....	62
46.3 Support Limitations	62
46.4 Recordkeeping.....	62
47. PLAYER INTERACTIONS, COMPLAINTS AND DISPUTES.....	63
47.1 Complaint Definition	63
47.2 Complaint Intake Channels.....	63
47.3 Complaint Logging	63
47.4 Complaint Categories.....	63
48. COMPLAINT INVESTIGATION AND INTERNAL ESCALATION	63
48.1 Fair Handling Principle	63
48.2 Complaint Investigation	64
48.3 Mandatory Escalation	64

48.4 Complaint Outcome	64
49. ADR AND EXTERNAL DISPUTE RESOLUTION	64
49.1 ADR Provider	64
49.2 Referral to ADR	64
49.3 ADR Case Handling	64
49.4 ADR Outcome Management.....	65
50. COMPLAINTS REGISTERS, REPORTING AND GOVERNANCE	65
50.1 Complaints Register	65
50.2 Complaints Reporting.....	65
50.3 Governance Review.....	65
INFORMATION SECURITY, ACCESS, CHANGE AND INCIDENT MANAGEMENT	66
51. INFORMATION SECURITY GOVERNANCE	66
51.1 Security Principle	66
51.2 Security Oversight	66
51.3 Relationship with Security Policy.....	66
52. ACCESS CONTROL, USER RIGHTS AND PRIVILEGED ACCESS	66
52.1 Access Restriction Principle.....	66
52.2 User Access Controls.....	66
52.3 Sensitive Systems	67
52.4 Shared Credentials	67
53. CHANGE MANAGEMENT, SYSTEM OVERRIDES AND OUTSOURCED DEVELOPMENT	67
53.1 Change Management Principle	67
53.2 Change Approval.....	67
53.3 System Overrides and Manual Workarounds	67
53.4 Outsourced Development / Supplier Changes	68
54. INCIDENT MANAGEMENT AND BREACH ESCALATION	68
54.1 Incident Definition	68
54.2 Incident Categories	68
54.3 Incident Response.....	68
54.4 Severity and Escalation	68
54.5 Incident Logging	69
55. REGULATORY, FIU AND LAW-ENFORCEMENT COOPERATION	69
55.1 Cooperation Obligation.....	69
55.2 Handling of Requests.....	69

55.3 Confidentiality and Recordkeeping	69
56. BUSINESS CONTINUITY AND DISASTER RECOVERY	69
56.1 Continuity Principle	69
56.2 Critical Processes.....	70
56.3 Contingency Planning.....	70
57. DIGITAL RECORDS AND DATA MANAGEMENT	70
58. Regulatory Incident Notification	71
58.1 Reportable Incidents	71
58.2 Regulatory Notification.....	71
58.3 Incident Management	71
59. Changes to this Operations Manual	72

VERSION CONTROL

Version	Date	Author / Owner	Summary of Changes	Approved By
1.0	26 June 2026	Craig Murugan	New	Board

1. PURPOSE OF THIS OPERATIONS MANUAL

1.1 PURPOSE

This Operations Manual sets out the governance framework, operational procedures, internal controls, escalation routes, decision-making authorities and day-to-day operating standards applicable to the online gaming operations conducted by **Surewin B.V** (the “**Company**”) under its Curaçao gaming License.

The purpose of this Manual is to ensure that **Surewin B.V** conducts its licensed gaming business in a controlled, transparent, secure and compliant manner and that all relevant staff, managers and service providers understand:

- their operational, control and escalation responsibilities;
- the procedures to be followed when onboarding, monitoring, restricting, paying, servicing or offboarding customers;
- the controls applicable to AML/CFT, sanctions, fraud, responsible gambling, complaints, security incidents and other material operational matters; and
- the records, approvals, registers and management information that must be maintained to demonstrate compliance with Curaçao Gaming Authority (“CGA”) requirements, applicable law and **Surewin B.V**'s internal control framework.

1.2 NATURE OF THIS MANUAL

This Manual is **Surewin B.V**'s primary operational implementation document for its licensed online gaming business. It translates legal, regulatory and policy obligations into practical operational procedures and control requirements.

It does not replace **Surewin B.V**'s:

- AML/CFT Policy;
- Responsible Gambling Policy;
- Complaints Handling Policy;
- Terms and Conditions;
- Information Security Policy; or
- any Board-approved specialist policy or regulatory procedure.

Instead, it must be read together with those documents and used as the principal operational reference for the day-to-day running of the licensed business.

1.3 OBJECTIVES

The objectives of this Manual are to:

- establish a clear and documented operating model for **Surewin B.V**'s;
- ensure customer onboarding, verification, monitoring, payments, complaints, responsible gambling and AML/CFT activities are performed consistently and in accordance with approved procedures;
- define approval requirements and escalation routes for high-risk, sensitive or exceptional matters;

- support accurate recordkeeping, auditability, management reporting and regulatory readiness; and
- support staff training, internal oversight and periodic control review.

2. SCOPE AND APPLICATION

2.1 SCOPE

This Manual applies to all online gaming operations conducted by **Surewin B.V** under its Curaçao License and/or Curaçao License application, including:

- online casino operations and any other approved gaming verticals operated under the Company's Curaçao License;
- customer registration, account opening, deposits, gameplay, withdrawals, account restriction and account closure;
- customer due diligence, enhanced due diligence and customer risk review;
- AML/CFT monitoring, sanctions screening, internal suspicious activity escalation and FIU reporting;
- fraud, chargeback, multiple-account and bonus abuse controls;
- responsible gambling monitoring, interventions, self-exclusion and vulnerable player handling;
- customer support, complaints, disputes and ADR handling;
- information security, access control, incident management and operational resilience; and
- outsourced or third-party service providers supporting the licensed operation.

2.2 WHO THIS MANUAL APPLIES TO:

This Manual applies to:

- Directors and senior management;
- the Compliance Officer;
- the MLRO;
- the Responsible Gambling Officer;
- customer support, risk, fraud, payments, finance, RG, compliance and operational staff;
- IT and security personnel; and
- temporary staff, contractors and outsourced service providers where they perform activities on behalf of the Company.

2.3 OBLIGATION TO COMPLY

All staff and relevant service providers must comply with this Manual and with all related policies, procedures and lawful internal instructions issued by **Surewin B.V**.

Failure to comply may result in:

- retraining and management intervention;
- withdrawal of access rights or operational authority;
- disciplinary action;

- escalation to the Compliance Officer, MLRO, Responsible Gambling Officer, Senior Management or Board; and
- where required, notification to regulators, law-enforcement agencies or other competent authorities.

3. REGULATORY FRAMEWORK

3.1 REGULATORY BASIS

The Company will operate in accordance with:

- the applicable Curaçao gaming licensing framework and any License conditions imposed by the Curaçao Gaming Authority;
- the National Ordinance on the Reporting of Unusual Transactions and any other applicable AML/CFT laws and implementing obligations in Curaçao;
- applicable sanctions legislation and related implementing measures;
- any applicable consumer protection, complaint-handling and ADR requirements relevant to licensed gaming operators;
- any other applicable laws, regulations, License conditions and regulatory guidance relevant to Surewin B.V's activities; and
- Surewin B.V's own Board-approved internal policies, procedures and control frameworks.

3.2 CORE REGULATORY AND CONTROL OBJECTIVES

Surewin B.V supports the following objectives:

- preventing the use of Surewin B.V's services for money laundering, terrorist financing, sanctions evasion, fraud or other criminal misuse;
- protecting players, including minors and vulnerable persons;
- ensuring fair, transparent and responsible treatment of customers;
- ensuring complaints are handled fairly, promptly and transparently;
- safeguarding operational integrity, information security and business continuity;
- maintaining complete records, audit trails and management oversight over the licensed business.

3.3 REGULATORY COOPERATION

Surewin B.V will cooperate with lawful requests, enquiries, inspections and reporting obligations involving the Curaçao Gaming Authority, the FIU, ADR bodies and law-enforcement authorities and will maintain records and procedures sufficient to support such cooperation.

4. RELATIONSHIP WITH OTHER POLICIES AND PROCEDURES

4.1 RELATED DOCUMENTS

This Manual must be read together with, at minimum, the following Surewin B.V documents:

- AML/CFT Policy and supporting AML procedures;
- Responsible Gambling Policy;
- Complaints Handling Policy;

- Terms and Conditions;
- Information Security / Cyber Security Policy;
- FIU / goAML reporting procedure or suspicious activity escalation procedure;
- Board-approved governance logs, registers, schedules and control documents.

4.2 HIERARCHY OF DOCUMENTS

Where a policy and this Manual overlap:

- the stricter requirement will apply;
- where a policy states what **Surewin B.V** must do and this Manual states how it must be done operationally, staff must comply with both; and
- where a conflict, ambiguity or gap is identified, the matter must be escalated to Compliance for clarification and, where relevant, to the MLRO or Responsible Gambling Officer.

4.3 SUPPORTING SOPS AND TEAM PROCEDURES

Surewin B.V maintains supporting SOPs, workflow notes, checklists, ticket-handling instructions or team procedures beneath this Manual. Any such document must remain consistent with this Manual and may not override any mandatory control, approval or escalation requirement set out herein.

5. DEFINITIONS

For the purposes of this Manual, unless the context requires otherwise:

- **Account** means a player account opened with **Surewin B.V** to access Surewin B.V's gaming services.
- **ADR** means alternative dispute resolution. **Surewin B.V**'s appointed ADR provider is **CADRE**.
- **AML/CFT** means anti-money laundering and counter-terrorist financing.
- **Board** means the **Surewin B.V**'s Board of Directors or equivalent governing body.
- **CGA** means the Curaçao Gaming Authority.
- **CDD** means customer due diligence.
- **Company** means **Surewin B.V**, the licensed or applicant operator to which this Manual applies.
- **Compliance Officer** means the person responsible for overseeing the Company's broader regulatory compliance framework, excluding matters specifically reserved for the MLRO.
- **Customer** or **Player** means any person holding or applying for an account with the Company.
- **EDD** means enhanced due diligence.
- **FIU** means the Financial Intelligence Unit Curaçao.
- **goAML** means the reporting platform used for submission of unusual transaction reports to the FIU.

- **MLRO** means the Money Laundering Reporting Officer.
- **PEP** means a politically exposed person.
- **RG** means responsible gambling / responsible gaming.
- **Source of Funds (SOF)** means the origin of funds used in relation to a customer's transactions with the Company.
- **Source of Wealth (SOW)** means the origin of a customer's accumulated wealth.
- **UTR** means an unusual transaction report / reportable unusual transaction under applicable law.

Additional definitions contained in the AML/CFT Policy, Responsible Gambling Policy, Complaints Handling Policy and Terms and Conditions will apply where relevant.

6. LICENSED ACTIVITIES

Surewin B.V conducts remote gaming operations under the applicable Curaçao License. The scope of licensed activities will be limited to those products, brands, websites and territories approved under the Company's licensing arrangements and internal governance approvals.

7. GOVERNANCE STRUCTURE AND OVERSIGHT

7.1 GOVERNANCE PRINCIPLE

Surewin B.V will maintain a governance structure that ensures effective oversight of gaming operations, AML/CFT, responsible gambling, complaints, player protection, operational resilience and outsourced service providers.

7.2 BOARD RESPONSIBILITY

The Board retains ultimate responsibility for ensuring that **Surewin B.V**:

- operates in compliance with the license obligations and applicable law;
- maintains an effective AML/CFT control framework;
- maintains appropriate responsible gambling controls and customer protection measures;
- allocates sufficient resources to compliance, AML, RG, complaints, risk and security functions;
- reviews material incidents, compliance breaches and regulatory reporting; and
- approves and periodically reviews key policies and this Operations Manual.

7.3 SENIOR MANAGEMENT OVERSIGHT

Senior Management is responsible for implementing this Manual and ensuring that operational controls are embedded in day-to-day practice. Senior Management must ensure that:

- business operations are adequately supervised;
- escalation routes are effective and understood;
- staff are trained and competent;
- control weaknesses are addressed promptly; and

- material incidents are escalated to the appropriate control function and, where necessary, to the Board.

7.4 CONTROL FUNCTIONS

Surewin B.V will maintain, whether internally or through approved outsourced arrangements, at minimum the following key control functions:

- Compliance Function;
- MLRO / AML Function;
- Responsible Gambling Function;
- Customer Support / Complaints Function;
- Risk / Fraud / Payments Control Function; and
- Information Security / IT Control Function.
- Data Protection Function

8. ROLES AND RESPONSIBILITIES

8.1 BOARD

The Board will:

- approve key compliance, AML, RG, complaints and security policies;
- review periodic management information and incident reporting;
- ensure the appointment of suitably qualified key function holders;
- ensure remedial action is taken where control deficiencies are identified; and
- ensure **Surewin B.V** maintains an appropriate operational framework for the licensed business.

8.2 MANAGING DIRECTOR / SENIOR MANAGEMENT

The Managing Director and/or delegated Senior Management will:

- ensure the licensed operation is run in accordance with this Manual;
- ensure sufficient staffing, systems and controls are in place;
- approve escalated operational decisions within delegated authority;
- ensure cooperation with the CGA, FIU, ADR bodies and law-enforcement authorities where required; and
- oversee remediation of material incidents, complaints, AML escalations and control weaknesses.

8.3 COMPLIANCE OFFICER

The Compliance Officer will:

- oversee the company's broader regulatory compliance framework;
- monitor implementation of this Manual and related policies;

- support policy updates, control reviews and remediation;
- oversee complaint, RG and operational compliance escalations not reserved for the MLRO; and
- support regulatory interactions and internal governance reporting.

8.4 MLRO

MLRO will:

- oversee the company's AML/CFT framework;
- review internal suspicious activity / unusual transaction escalations;
- determine whether a UTR must be filed with the FIU;
- maintain the MLRO investigation register and related AML records;
- report material AML matters to Senior Management and/or the Board; and
- support AML training, control reviews and regulatory engagement on AML matters.

8.5 RESPONSIBLE GAMBLING OFFICER

The Responsible Gambling Officer will:

- oversee **Surewin B.V.**'s responsible gambling framework;
- review and direct interventions for vulnerable or at-risk customers;
- oversee self-exclusion, cooling-off, operator-imposed restrictions and RG reporting;
- liaise with support, compliance and management on serious RG concerns; and
- ensure RG interactions, decisions and restrictions are appropriately recorded.

8.6 CUSTOMER SUPPORT / OPERATIONS MANAGER

The Customer Support / Operations Manager will:

- oversee day-to-day player communications and support operations;
- ensure customer queries, complaints and escalations are logged and actioned appropriately;
- ensure support staff escalate AML, RG, fraud and payment concerns in accordance with this Manual; and
- maintain service standards and complaint-routing discipline.

8.7 RISK / FRAUD / PAYMENTS OWNER

The Risk / Fraud / Payments Owner will:

- oversee payment processing, withdrawal review and payment-related controls;
- review fraud, multiple-account, chargeback and bonus abuse concerns;
- ensure withdrawal releases are supported by required approvals;
- maintain controls over refunds, reversals and manual balance adjustments; and
- liaise with Compliance and the MLRO where payment activity creates AML concerns.

8.8 FINANCE / RECONCILIATION OWNER

The Finance / Reconciliation Owner will:

- support reconciliation of player liabilities, wallets and payment settlements;
- support financial recordkeeping and payment investigations;
- assist with the control of manual adjustments and financial exception handling; and
- escalate discrepancies or unexplained movements to the appropriate control function.

8.9 IT / SECURITY OWNER

The IT / Security Owner will:

- oversee access control, security monitoring, change management and incident response;
- ensure licensed systems and player data are appropriately protected;
- support evidence preservation, access investigations and business continuity arrangements; and
- coordinate with outsourced technical providers where applicable.

8.10 ALL EMPLOYEES

All employees must:

- comply with this Manual and related policies;
- escalate suspicious, unusual, harmful or high-risk customer behaviour;
- keep accurate and timely case notes;
- cooperate with investigations, reviews, control testing; and
- avoid tipping off customers in AML matters or taking unauthorized decisions outside their delegated authority.

9. DELEGATED AUTHORITY AND APPROVAL FRAMEWORK

9.1 PRINCIPLE

Surewin B.V will maintain a delegated authority framework so that high-risk, sensitive or exceptional matters are reviewed and approved by appropriate senior personnel and, where relevant, the appropriate control functions.

9.2 MATTERS REQUIRING ESCALATED APPROVAL

At a minimum, the following matters must be escalated for approval in accordance with **Surewin B.V**'s Approval Matrix:

- approval or retention of high-risk customers following EDD;
- onboarding or retention of PEPs;
- sanctions or true-match screening escalations;

- confiscation of funds or bonus balances due to fraud, multi-accounting or serious Terms breaches;
- manual override of standard withdrawal controls;
- material goodwill, settlement or complaint compensation decisions;
- operator-imposed exclusion or serious RG intervention decisions;
- reporting of material incidents to the CGA or FIU; and
- approval of policy exceptions or temporary control workarounds.

9.3 APPROVAL MATRIX

A formal Approval Matrix will be maintained and will identify:

- the decision type;
- the primary reviewer;
- the approving role;
- any second-line or control review requirement;
- whether Senior Management or Board notification is required; and
- the register, log or case note in which the decision must be recorded.

10. WHISTLEBLOWING AND PROTECTED DISCLOSURES

10.1 PRINCIPLE

Surewin B.V encourages employees and relevant service providers to report genuine concerns regarding misconduct, illegal activity, breaches of law, regulatory non-compliance, AML failures, player protection failures, unethical behaviour, fraud, corruption or serious control weaknesses.

10.2 NO RETALIATION

No employee will be penalized, dismissed, disadvantaged or retaliated against for making a genuine report of wrongdoing in good faith, even if the concern is not ultimately substantiated.

10.3 MATTERS THAT MAY BE REPORTED

Concerns that may be reported under this section include:

- suspected money laundering, sanctions evasion or suspicious activity not being escalated properly;
- deliberate bypassing of RG controls or self-exclusion restrictions;
- falsification of records, documents or approvals;
- deliberate payment or withdrawal control circumvention;
- customer or staff fraud;
- unauthorized system access or security misconduct; and
- harassment, intimidation or attempts to suppress legitimate reporting.

10.4 REPORTING CHANNELS

Concerns may be reported to one or more of the following, depending on the nature of the concern:

- line management;
- the Compliance Officer;
- the MLRO;
- the Responsible Gambling Officer;
- Senior Management or the Board; or
- any dedicated whistleblowing channel adopted by **Surewin B.V.**

10.5 CONFIDENTIALITY

Reports should be handled confidentially to the fullest extent possible, subject to legal, regulatory or investigative requirements.

10.6 RECORDKEEPING

Whistleblowing reports, outcomes and any resulting remediation actions should be recorded in a secure and access-controlled manner.

11. DOCUMENT GOVERNANCE AND REVIEW CYCLE

11.1 DOCUMENT OWNERSHIP

This Manual is owned by Compliance in conjunction with Operations and the MLRO for AML/CFT sections. Section owners may be designated for specialist chapters, including RG, complaints, payments and information security.

11.2 REVIEW FREQUENCY

This Manual will be reviewed:

- at least annually;
- upon material regulatory change;
- following any material incident, enforcement issue, control failure or significant business change; and
- when new products, payment methods, systems or outsourced service providers are introduced.

11.3 VERSION CONTROL

Surewin B.V. will maintain version control for this Manual and all related policies, including:

- version number;
- effective date;
- summary of changes;

- approver; and
- next review date.

11.4 CONTROLLED COPIES

Only the latest approved version of this Manual may be used for operational purposes. Historic versions must be archived but clearly marked as superseded.

12. BUSINESS OVERVIEW

12.1 BUSINESS MODEL

Surewin B.V operates an online gaming business under the Curaçao License and/or Curaçao application framework. **Surewin B.V** offers remote gaming products through its approved websites and brands and services customers in approved jurisdictions only.

12.2 CORE OPERATING FUNCTIONS

Surewin B.V's operating model includes the following core functions:

- customer registration and account management;
- KYC, CDD and EDD;
- payments, withdrawals and reconciliations;
- fraud and transaction monitoring;
- AML/CFT monitoring and reporting;
- responsible gambling monitoring and interventions;
- customer support and complaints handling; and
- IT, information security and operational resilience.

12.3 PLAYER LIFECYCLE OVERVIEW

Surewin B.V's player lifecycle includes:

- registration and account creation;
- initial screening and acceptance controls;
- deposit and gameplay activity;
- ongoing monitoring for AML, RG, fraud and behavioural risks;
- withdrawal processing and enhanced checks where triggered; and
- complaint handling, restrictions, suspension, self-exclusion or account closure where required.

12.4 GAMING OPERATIONS, PRODUCTS AND SERVICES

12.4.1 Purpose

This section describes **Surewin B.V**'s gaming operations, products and services and forms part of **Surewin B.V**'s Operations Manual maintained in accordance with Article 5.9 of the National Ordinance on Games of Chance (LOK). It outlines the products offered, software standards, payment facilities, wagering principles, payout processes and game integrity controls

implemented to ensure the fair, secure and compliant operation of Surewin B.V's online gaming business.

12.4.2 Gaming Products

Surewin B.V operates an online casino platform and may offer one or more of the following licensed Games of Chance:

- Online Slot Games
- Live Dealer Casino Games
- Table Games
- Instant Win Games
- Progressive Jackpot Games
- Promotional Tournament Games
- Other games approved under Surewin B.V's Gaming License.

No game will be made available unless it has successfully completed Surewin B.V's commercial, technical, security and compliance onboarding process.

12.4.3 Software Providers

Gaming content will only be supplied by approved software providers that meet Surewin B.V's due diligence requirements.

Prior to integration, Surewin B.V will assess:

- licensing and regulatory status;
- technical compatibility;
- contractual arrangements;
- information security standards;
- game certification (where applicable);
- operational readiness; and
- ongoing support capabilities.

Surewin B.V will maintain a Gaming Provider Register recording the approval status of each integrated provider.

12.4.4 Outcome Determination and Fair Gaming

Game outcomes will be determined exclusively through certified Random Number Generator (RNG) technology or authorised live gaming systems operated by approved gaming providers.

Surewin B.V will not manipulate, interfere with or influence game outcomes, return-to-player settings or game mathematics.

Only games independently tested and certified, where certification is required, will be offered.

12.4.5 Betting Parameters

Minimum and maximum betting limits will be configured within the gaming platform and may vary according to:

- individual game configuration;
- promotional campaigns;
- player risk profile;
- responsible gambling controls;
- applicable legal or regulatory requirements.

12.4.6 Payment Facilities

Customers may deposit and withdraw using payment methods approved by Surewin B.V including, where available:

- debit cards;
- approved electronic wallets;
- alternative payment methods; and
- other approved payment solutions.

All payment methods are subject to operational, fraud, AML/CFT and security controls.

12.4.7 Withdrawal Controls

Before a withdrawal is approved, Surewin B.V will complete, where applicable:

- customer identity verification;
- payment ownership verification;
- AML/CFT review;
- sanctions screening;
- fraud review;
- responsible gambling review;
- Enhanced Due Diligence;
- Source of Funds review.

Withdrawal processing is governed by the Withdrawal Procedure contained within this Operations Manual and supported by the AML/CFT Policy.

12.5 GAMES OF CHANCE, BETTING AND OUTCOME DETERMINATION

12.5.1 Games Offered

Surewin B.V operates an online casino platform offering Games of Chance supplied by licensed and approved third-party gaming providers. The portfolio may include, subject to commercial availability and regulatory approval:

- Online Slot Games;
- Live Dealer Casino Games;
- Roulette;
- Blackjack;
- Baccarat;
- Poker Variants;
- Game Shows;
- Instant Win Games; and

- other certified casino games made available through approved gaming suppliers.

The range of games available to players may change from time to time depending on supplier agreements, commercial decisions and regulatory requirements.

12.5.2 Software Providers

All Games of Chance are supplied by reputable third-party gaming providers operating under appropriate licences and certifications. Surewin B.V does not alter, manipulate or influence the software, game mathematics or outcome logic provided by certified game suppliers.

12.5.3 Outcome Determination

Game outcomes are determined exclusively by:

- certified Random Number Generator (RNG) technology for RNG-based games; or
- real-time live gaming activity for Live Dealer games, as implemented and controlled by the respective certified gaming providers.

Surewin B.V has no ability to influence, modify or predetermine the outcome of any game.

12.5.4 Betting Limits and Payouts

Minimum and maximum betting limits are established within each individual game by the relevant gaming provider and may vary between products.

Player winnings are calculated automatically by the certified game software in accordance with the published game rules and pay tables applicable to each game.

Approved winnings are credited automatically to the player's gaming wallet following completion of the game, subject to any applicable regulatory, fraud prevention, AML/CFT or operational review requirements.

12.5.5 Return to Player

Where applicable, the theoretical Return to Player (RTP) percentages for games are determined by the certified game providers and are made available to players in accordance with supplier specifications and applicable regulatory requirements.

12.6 PLAYER WEBSITE AND INTERFACE

12.6.1 Overview

Surewin B.V provides its Games of Chance through a secure online gaming website and, where applicable, compatible mobile interfaces. The player interface is designed to provide a clear, transparent and user-friendly experience while supporting regulatory compliance, responsible gambling and customer protection requirements.

The website will present information in a clear and accessible manner and will provide players with access to all essential account management and regulatory information.

12.6.2 Player Interface

The player interface may include, where applicable:

- player registration and account creation;
- secure login and authentication;
- account verification and KYC notifications;
- player profile and account management;
- deposit and withdrawal facilities;
- gaming lobby and game selection;
- account balance and transaction history;
- bonus and promotional information;
- responsible gambling tools, including deposit limits, loss limits, cooling-off and self-exclusion;
- customer support and contact information;
- complaints submission channels;
- General Terms and Conditions;
- Privacy Policy;
- Responsible Gambling information;
- AML and verification notices where applicable; and
- other information necessary to support the safe operation of the licensed gaming activities.

12.6.3 Responsible Gambling Information

The website will prominently display responsible gambling information and provide players with access to responsible gambling tools and educational material.

Where appropriate, players will also receive system-generated notifications relating to responsible gambling, account verification, regulatory requirements or operational restrictions.

12.6.4 Customer Information

The website will clearly communicate:

- applicable Terms and Conditions;
- bonus terms, where offered;
- payment methods;
- account verification requirements;
- withdrawal procedures;
- complaint escalation procedures;
- responsible gambling contacts; and
- other regulatory disclosures required under applicable laws and license conditions.

12.6.5 Ongoing Review

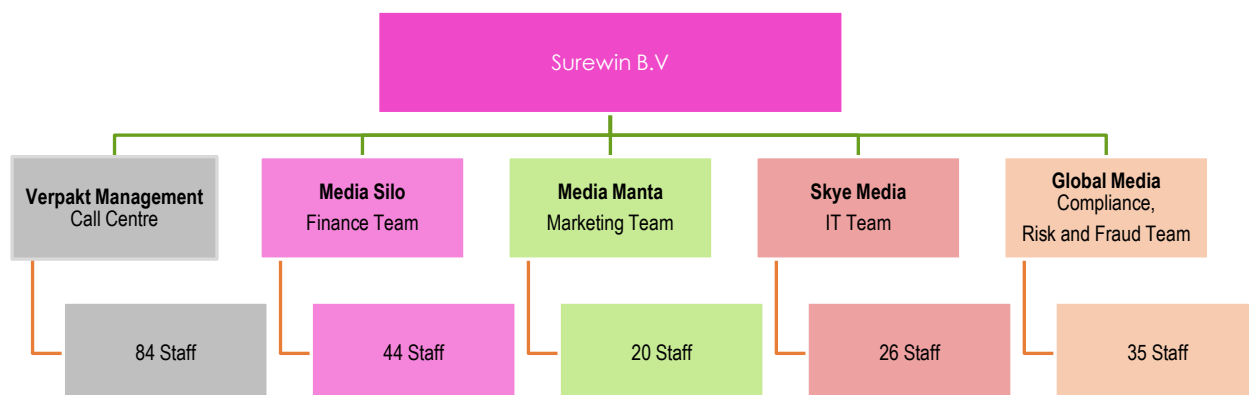
Surewin B.V will periodically review the player interface to ensure that information remains accurate, accessible and compliant with applicable regulatory requirements. Material changes to the player interface will be subject to **Surewin B.V**'s change management and governance procedures.

13. ORGANISATIONAL STRUCTURE AND DEPARTMENTS

13.1 ORGANISATIONAL STRUCTURE



OPERATIONAL STRUCTURE



13.2 DEPARTMENTAL COORDINATION

Operational effectiveness requires coordination between support, risk, fraud, payments, AML, RG, compliance and IT teams. Matters that create cross-functional risks such as suspicious withdrawals, vulnerable customer complaints, sanction matches, fraud rings or security incidents must be escalated to all relevant stakeholders rather than handled in isolation.

14. CRITICAL SYSTEMS, PLATFORMS AND TOOLS

14.1 SYSTEM REGISTER

Surewin B.V. will maintain a register of all critical systems used in the licensed operation, including:

- the player account management / gaming platform;
- KYC / verification systems;
- PEP / sanctions / adverse media screening tools;
- fraud monitoring tools;
- payment gateway and PSP systems;
- complaint and support ticketing systems;
- RG monitoring tools and self-exclusion records;
- secure document storage and case management systems; and
- FIU goAML reporting access credentials and procedures.

14.2 ACCESS PRINCIPLE

System access will be role-based and granted only to authorized personnel with a legitimate operational need.

14.3 SYSTEM DEPENDENCIES

Surewin B.V will identify critical system dependencies and maintain awareness of which outsourced or internal functions rely on each system for customer onboarding, withdrawals, RG controls, AML reviews, complaint handling and reporting.

14.4 TECHNICAL INFRASTRUCTURE OVERVIEW

Surewin B.V maintains secure technical infrastructure supporting all licensed gaming activities.

The operational environment consists of:

- customer-facing gaming website;
- Player Account Management (PAM) platform;
- gaming content providers;
- payment service providers;
- customer verification services;
- AML/CFT monitoring systems;
- fraud monitoring solutions;
- responsible gambling controls;
- customer relationship management systems;
- reporting and audit systems; and
- secure hosting infrastructure. EDR(CrowdStrike), Vulnerability Management, SOC (SJ), backups/Syncing, Web and application filtering, DDOS (Cloudflare and FortiGate)
- Secure Private cloud hosting

The infrastructure is designed to support confidentiality, integrity, availability and resilience of all critical gaming operations.

14.5 TECHNICAL INFRASTRUCTURE DIAGRAM



Surewin B.V maintains:

- encrypted communications; TLS
- role-based access controls;
- network monitoring; Firewalls, EDR (CrowdStrike), Server monitoring (ES, Local Zabbix)
- regular backups; ES backups, DR site, DB syncing
- disaster recovery procedures; L:\Documentation\Wiki's\Security\Policies\Blanks\Business Continuity Disaster Recovery Procedures.docx
- business continuity arrangements;
L:\Documentation\Wiki's\Security\Policies\Blanks\Business Continuity Disaster Recovery Procedures.docx
- restoration testing; and File and data restoration is done on request.
- incident response procedures. L:\Documentation\Wiki's\Security\Policies\Blanks\Security Incident Management.docx

15. OUTSOURCING AND CRITICAL SUPPLIER OVERSIGHT

15.1 OUTSOURCING PRINCIPLE

Where Surewin B.V outsources part of its licensed operation to third-party service providers, Surewin B.V remains responsible for ensuring that outsourced activities are performed in a compliant and controlled manner.

15.2 CRITICAL SUPPLIERS

Critical suppliers may include:

- platform / PAM providers;
- payment service providers;
- screening vendors;
- game providers;
- hosting and IT providers;
- outsourced MLRO; and
- the ADR provider.

15.3 OVERSIGHT REQUIREMENTS

For each critical supplier, **Surewin B.V** will maintain:

- a record of services provided;
- the responsible internal owner;
- contractual and service oversight arrangements;
- incident escalation and business continuity contacts; and
- periodic review of supplier performance and compliance relevance.

15.4 OPERATIONAL QUALITY MONITORING AND TESTING

15.4.1 Principle

Surewin B.V will maintain a documented programme of operational quality monitoring to verify that its operational procedures, internal controls and regulatory obligations continue to operate effectively. The programme is designed to identify control deficiencies, operational weaknesses, process failures and opportunities for continuous improvement.

15.4.2 Scope of Quality Monitoring

Operational quality monitoring will include periodic reviews of, at a minimum:

- customer registration and onboarding procedures;
- customer due diligence (CDD), KYC and enhanced due diligence (EDD) controls;
- payment processing, deposits and withdrawals;
- fraud prevention and transaction monitoring;
- responsible gambling controls and customer interaction procedures;
- complaints handling and dispute resolution;
- information security and access management controls;
- supplier performance and outsourced service delivery;
- business continuity and disaster recovery arrangements; and
- compliance with applicable laws, license conditions, internal policies and standard operating procedures.

15.4.3 Monitoring Methods

Quality monitoring may include one or more of the following methods:

- file and transaction sampling;

- management quality assurance reviews;
- operational KPI and SLA monitoring;
- compliance monitoring reviews;
- internal audits;
- supplier performance reviews;
- reconciliation testing;
- system access and user permission reviews;
- incident trend analysis;
- complaint trend analysis;
- responsible gambling monitoring; and
- corrective action follow-up reviews.

15.4.4 Frequency

Quality monitoring activities will be performed on a risk-based basis and may be conducted daily, weekly, monthly, quarterly or annually depending on the nature of the operational control being reviewed.

Higher-risk operational areas will be reviewed more frequently.

15.4.5 Reporting and Continuous Improvement

Material findings identified through quality monitoring will be documented, assigned to the appropriate business owner and tracked through to completion.

Where deficiencies are identified, corrective actions will be implemented within reasonable timeframes. Management will periodically review quality monitoring outcomes to assess control effectiveness, identify recurring issues and support continuous operational improvement.

16. CUSTOMER REGISTRATION AND ACCOUNT OPENING - PLAYER ACCOUNT LIFECYCLE OPERATIONS

16.1 ACCOUNT REGISTRATION

A player may open an account only through **Surewin B.V**'s approved registration process. At registration, **Surewin B.V** will collect the minimum information required under applicable law, licensing requirements and internal risk controls, which may include:

- full name;
- date of birth;
- residential address;
- email address and contact details;
- country of residence;
- payment details where relevant; and
- any other information reasonably required for KYC, fraud prevention or RG controls.

16.2 AGE AND ELIGIBILITY GATE

No account may be accepted where:

- the customer is under the legal minimum age;

- the customer is located in, or resident in a prohibited jurisdiction;
- the customer appears on sanctions lists or is otherwise prohibited from receiving Surewin B.V's services; or
- Surewin B.V cannot satisfy itself that the customer may lawfully use the service.

16.3 INITIAL SCREENING

Surewin B.V will conduct, either at registration or before the account becomes fully operational, screening and validation checks including as applicable:

- sanctions / PEP / adverse media screening;
- duplicate account screening;
- geolocation or jurisdiction controls;
- fraud or behavioural risk checks; and
- review of unusual registration patterns or device indicators.

16.4 MANUAL REVIEW TRIGGERS AT ONBOARDING

An account must be referred to for manual review where there are indicators including:

- inconsistent registration information;
- duplicate or linked account indicators;
- restricted jurisdiction concerns;
- sanctions / PEP / adverse media alerts;
- unusual device, IP, payment or behavioural indicators; or
- suspected underage play or false identity.

17. CUSTOMER DUE DILIGENCE / KYC PROCEDURE

17.1 KYC OBLIGATION

Surewin B.V will conduct customer due diligence in accordance with applicable AML/CFT law, its AML/CFT Policy and this Manual. CDD may be performed before, during or after registration depending on the customer risk profile, transaction activity and applicable legal thresholds, but must always be completed before Surewin B.V permits activity inconsistent with its AML obligations.

17.2 STANDARD KYC INFORMATION AND DOCUMENTS

CDD may include collection and verification of:

- proof of identity;
- proof of address;
- date of birth verification;
- payment method ownership evidence;
- occupation or source of funds, information where required; and
- any additional documentation needed to understand the customer relationship.

17.3 TRIGGER EVENTS FOR KYC REVIEW

Surewin B.V will perform or refresh KYC/CDD where triggered by:

- the establishment of a business relationship;
- cumulative deposit / transaction thresholds under applicable law or policy;
- withdrawal requests where verification has not yet been completed;
- suspicious, unusual or inconsistent activity;
- a change in customer risk profile;
- account inactivity followed by unusual reactivation patterns; or
- sanctions, PEP or adverse media developments.

17.4 KYC WORKFLOW

Where KYC is triggered:

1. the account will be placed in the relevant review queue;
2. the customer will be requested to provide the required documents and/or information;
3. the account may be restricted from deposits, withdrawals, gameplay or certain features until review is complete;
4. the reviewer will assess the documents, data consistency, payment ownership, jurisdiction and risk indicators;
5. the reviewer will record the outcome, rationale and any escalation; and
6. if unresolved or unsatisfactory, the matter will be escalated to Compliance, AML, Risk or RG as appropriate.

17.5 FAILURE TO COMPLETE VERIFICATION

Where the customer fails to provide required information or documents within the period stipulated by Surewin B.V's AML/CFT Policy or operational request, Surewin B.V may:

- suspend or restrict the account;
- refuse or delay withdrawals pending satisfactory verification;
- terminate the business relationship; or
- return or withhold funds only in accordance with applicable law, AML obligations and internal approval requirements.

18. ENHANCED DUE DILIGENCE, SOURCE OF FUNDS, SOURCE OF WEALTH AND BENEFICIAL OWNERSHIP

18.1 EDD REQUIREMENT

Enhanced due diligence will be applied where the customer or activity presents heightened ML/TF, sanctions, fraud or regulatory risk. EDD may be triggered by:

- high or unusual transaction volumes;
- high-risk jurisdiction indicators;

- PEP status;
- unusual gameplay, deposit or withdrawal patterns;
- linked transactions or structuring indicators;
- adverse media, criminal intelligence or law-enforcement interest; or
- any other risk factor identified by the company.

18.2 EDD MEASURES

EDD may include:

- obtaining additional identity information;
- obtaining source of funds and/or source of wealth evidence;
- understanding the purpose and nature of the customer relationship;
- obtaining additional information on occupation, business activity, ownership or wealth profile;
- obtaining management or MLRO approval to continue the relationship; and
- applying enhanced monitoring and periodic review.

18.3 SOURCE OF FUNDS / SOURCE OF WEALTH REVIEW

Where SOF or SOW is required, the reviewer will:

- request documents or information reasonably sufficient to explain the origin of funds and/or wealth;
- assess whether the information is plausible, consistent and proportionate to the customer's activity;
- record the evidence reviewed, conclusions reached and any follow-up action; and
- escalate any inadequacy, inconsistency or suspicion to the MLRO and/or Compliance.

18.4 BENEFICIAL OWNERSHIP / THIRD-PARTY FUNDING CONCERNS

Where there are indicators that the account may be funded or controlled by a third party, or where beneficial ownership concerns arise, the matter must be escalated for enhanced review. **Surewin B.V** may request additional documentation, explanations or declarations and may restrict the account pending satisfactory resolution.

19. PEP, SANCTIONS AND ADVERSE MEDIA SCREENING

19.1 SCREENING REQUIREMENT

Surewin B.V will screen customers against sanctions, PEP and adverse media sources in accordance with the AML/CFT Policy and any approved system configuration.

19.2 POSITIVE MATCH HANDLING

Where a screening alert is generated:

- the alert must be reviewed by an authorized person;

- false positives must be documented and closed with rationale;
- potential true matches must be escalated to Compliance and/or the MLRO without delay;
- the account may be restricted while the alert is under review; and
- no account may proceed where sanctions exposure is confirmed unless permitted by law and approved through the appropriate escalation process.

19.3 PEP CUSTOMERS

Customers identified as PEPs, or close associates / family members where relevant, must be subject to enhanced due diligence, management approval and enhanced monitoring in accordance with the AML/CFT Policy.

20. RESTRICTED JURISDICTIONS AND PROHIBITED CUSTOMERS

20.1 RESTRICTED JURISDICTION CONTROLS

Surewin B.V will not knowingly accept or retain customers from jurisdictions where:

- **Surewin B.V** is not authorized to offer services;
- sanctions or legal restrictions prohibit the service; or
- the Company's internal risk appetite prohibits acceptance.

20.2 DETECTION AND ESCALATION

Indicators of restricted jurisdiction or prohibited use include:

- mismatched address, IP, payment and device information;
- use of anonymizing tools, proxies or suspicious VPN activity where prohibited;
- conflicting declarations of residence or location; or
- payment instruments linked to prohibited geographies.

Where such indicators arise, the account must be reviewed and may be restricted or closed.

21. ACCOUNT RESTRICTIONS, SUSPENSION, BLOCKING AND CLOSURE

21.1 GROUNDS FOR RESTRICTION OR SUSPENSION

Surewin B.V may restrict, suspend or block an account where there are concerns relating to:

- incomplete KYC / EDD;
- suspected fraud, multi-accounting or payment abuse;
- suspicious or unusual transactions;
- sanctions or PEP escalation;
- underage gambling concerns;
- responsible gambling concerns;
- material breach of Terms and Conditions; or

- law-enforcement or regulatory instructions.

21.2 OPERATIONAL CONTROLS

When an account is restricted or suspended:

- the reason must be recorded internally;
- the account status and any transactional restrictions must be updated in the relevant system;
- the matter must be escalated to the appropriate control function where required; and
- communications to the customer must be controlled and must not amount to tipping off in AML cases.

21.3 ACCOUNT CLOSURE

Accounts may be closed voluntarily by the customer or involuntarily by **Surewin B.V** in accordance with law, the Terms and Conditions, AML obligations, RG obligations or operational risk concerns.

22. DORMANT ACCOUNTS AND REACTIVATION

22.1 DORMANCY

Dormant accounts will be handled in accordance with **Surewin B.V**'s Terms and Conditions and applicable law. **Surewin B.V** will maintain controls for:

- identification of dormant accounts;
- customer notification where required;
- restriction or reactivation of dormant accounts; and
- treatment of balances and recordkeeping.

22.2 REACTIVATION

Where a dormant account is reactivated, **Surewin B.V** may require refreshed KYC, payment verification, fraud review or RG review before permitting further use.

23. DEPOSIT ACCEPTANCE CONTROLS

23.1 PURPOSE

This Part sets out the operational controls governing deposits, player funds, withdrawal processing, fraud prevention, chargeback handling, manual adjustments and related payment controls applicable to **Surewin B.V**'s licensed gaming operation.

23.2 DEPOSIT ACCEPTANCE PRINCIPLE

Surewin B.V will accept deposits only from customers who:

- have opened an account in accordance with this Manual;

- are not restricted, suspended, self-excluded or otherwise prohibited from using the service; and
- are using approved payment methods in accordance with Surewin B.V's internal controls, Terms and Conditions and applicable law.

23.3 PAYMENT METHOD CONTROLS

Surewin B.V will maintain controls designed to ensure that:

- payment methods used on the account belong to, or are legitimately controlled by, the customer;
- payment methods are not used in a manner that creates fraud, AML, RG or third-party funding concerns;
- payment transactions are monitored for irregular, excessive, unusual or inconsistent activity; and
- deposits are accepted only through approved payment channels and methods supported by Surewin B.V.

23.4 DEPOSIT MONITORING

Deposits must be monitored for indicators including:

- unusual value, volume or velocity;
- rapid increases in spending are inconsistent with the customer's known or expected profile;
- repeated failed deposits or repeated use of multiple cards, wallets or payment methods;
- possible third-party payment use;
- suspicious, linked or structured transactions; and
- fraud, chargeback or bonus abuse risk.

23.5 DEPOSIT RESTRICTIONS

Surewin B.V may refuse, reverse, delay or restrict a deposit where:

- the customer has not completed required verification;
- the payment appears to originate from an unauthorized, suspicious or unexplained source;
- fraud, AML, RG or sanctions concerns exist;
- the customer is located in a prohibited jurisdiction; or
- acceptance of the deposit would otherwise breach law, policy, the Terms and Conditions or internal risk controls.

23.6 RECORDKEEPING

Payment activity, holds, reversals, restrictions and related decisions must be recorded in the relevant payment, risk, AML or case management records.

24. PLAYER FUNDS, WALLETS AND BALANCE CONTROLS

24.1 PLAYER BALANCE INTEGRITY

Surewin B.V will maintain accurate records of player balances, deposits, withdrawals, bonuses, manual adjustments and any applicable fees or deductions in accordance with applicable law, license conditions and internal controls.

24.2 WALLET AND LEDGER CONTROLS

Surewin B.V will ensure that:

- player wallets or balance records are updated accurately and promptly;
- all balance movements are supported by a valid transaction, approved adjustment or documented system event;
- access to wallet adjustment functionality is restricted to authorized personnel; and
- adjustments, reversals and exceptions are subject to appropriate review and approval.

24.3 SEGREGATION OF DUTIES

Where operationally possible, **Surewin B.V** will separate:

- customer support handling from financial approval authority;
- payment review from AML approval functions;
- manual adjustment initiation from approval; and
- reconciliation from front-line transaction processing.

24.4 RECONCILIATIONS AND EXCEPTION REVIEW

Surewin B.V will maintain periodic reconciliations and exception review processes to identify:

- unexplained balance discrepancies;
- duplicate payments, duplicate credits or unexplained reversals;
- failed or delayed withdrawal issues;
- manual adjustment anomalies; and
- PSP or system-related transaction mismatches.

Any material discrepancy must be escalated to the relevant owner and, where appropriate, to Finance, Risk, Compliance, AML or Senior Management.

25. WITHDRAWAL REVIEW AND APPROVAL PROCEDURE

25.1 WITHDRAWAL REVIEW PRINCIPLE

No withdrawal will be released unless **Surewin B.V**'s withdrawal review process has been completed. That process must include verification of customer status, KYC status, payment method legitimacy and any AML, fraud, RG or sanctions considerations triggered by the customer's activity.

25.2 STANDARD WITHDRAWAL REVIEW

Upon receipt of a withdrawal request, the reviewer must, at minimum, consider:

- whether the customer's account is active and not suspended, blocked or under restriction;
- whether KYC / CDD requirements have been completed or triggered;
- whether the payment method and requested destination are permitted, legitimate and appropriate;
- whether the withdrawal amount, transaction history or customer behaviour gives rise to fraud, AML or RG concern;
- whether there are linked accounts, chargebacks, bonus abuse flags or payment disputes on file; and
- whether there are pending complaints, account closure issues or operational notes relevant to the payment.

25.3 WITHDRAWAL HOLD OR ESCALATION TRIGGERS

A withdrawal must be placed on hold and escalated where one or more of the following apply:

- KYC / EDD is incomplete, unsatisfactory or under review;
- the customer has triggered source of funds / source of wealth review;
- there are linked transactions or structuring indicators;
- there is suspected fraud, multi-accounting, chargeback or payment abuse;
- the customer is under AML review, RG review or sanctions review;
- the payment destination is new, unexplained or appears to belong to a third party; or
- the customer's behaviour or account history otherwise creates a material risk concern.

25.4 APPROVAL AND RELEASE

Where no material concerns remain and all required checks are complete, the withdrawal may be approved and released by an authorized reviewer in accordance with [Surewin B.V's](#) Approval Matrix.

25.5 REJECTION, REFUSAL OR CONFISCATION

A withdrawal may only be refused, delayed, returned or confiscated where:

- the Company is legally entitled or required to do so;
- the Company's Terms and Conditions and internal controls support the action;
- the decision has been reviewed and approved at the appropriate level; and
- the rationale is fully documented.

25.6 WITHDRAWAL RECORDKEEPING

The reviewer must document:

- the date and amount of the withdrawal;
- the checks performed;
- documents reviewed;
- whether the case was escalated;
- the outcome and rationale; and
- the approving person where required.

26. UNWAGERED DEPOSITS, WITHDRAWAL HOLDS AND SOURCE OF FUNDS REVIEWS

26.1 UNWAGERED OR MINIMALLY USED FUNDS

Where a customer seeks to withdraw un-wagered or minimally used deposited funds, Surewin B.V assesses, the request in light of:

- Terms and Conditions;
- the customer's KYC / EDD status;
- fraud and payment method legitimacy; and
- potential AML concerns, including whether the account may be used to move funds rather than gamble.

26.2 SOURCE OF FUNDS AND PURPOSE REVIEW

Surewin B.V may require source of funds information or additional explanation where:

- deposits are high, unusual or inconsistent with the customer's profile;
- a customer deposits and withdraws with little or no genuine gaming activity;
- there is repeated cycling of funds through the account; or
- the customer's behaviour suggests possible use of the platform for fund movement, layering or other suspicious activity.

26.3 WITHDRAWAL HOLDS PENDING REVIEW

A withdrawal may remain on hold pending:

- receipt of KYC / EDD / SOF documents;
- completion of fraud or chargeback checks;
- MLRO or Compliance review;
- RG review where relevant to account restriction; and
- internal management approval where required by the Approval Matrix.

27. FRAUD, MULTIPLE ACCOUNTS, CHARGEBACKS AND BONUS ABUSE

27.1 FRAUD PREVENTION OBJECTIVE

Surewin B.V will maintain operational controls designed to detect and prevent fraud, chargebacks, multiple-account misuse, identity misuse, bonus abuse, payment abuse and other dishonest or prohibited conduct.

27.2 FRAUD INDICATORS

Indicators of fraud or abuse may include:

- use of multiple accounts by the same individual or linked individuals;
- shared devices, IPs, payment methods, addresses or other identifiers across accounts;
- chargeback behaviour or payment disputes inconsistent with legitimate use;
- mismatched customer identity and payment ownership details;
- bonus abuse patterns, arbitrage behaviour or collusive behaviour; and
- suspicious deposit and withdrawal patterns inconsistent with normal gaming use.

27.3 FRAUD REVIEW ACTIONS

Where fraud or abuse indicators arise, **Surewin B.V** may:

- place the account under review;
- request additional verification or payment ownership evidence;
- restrict deposits, gameplay or withdrawals;
- reverse bonuses or promotional benefits where permitted by the Terms and Conditions;
- close or block the account; and
- escalate to AML, Compliance or the MLRO where criminal or suspicious fund movement concerns exist.

27.4 CHARGEBACK HANDLING

Chargebacks and payment disputes must be logged and reviewed to determine:

- whether the transaction is genuine, mistaken or fraudulent;
- whether linked accounts or payment methods are affected;
- whether the customer relationship should be restricted or terminated; and
- whether the matter gives rise to AML, fraud or law-enforcement escalation.

27.5 CONFISCATION / FORFEITURE DECISIONS

Any confiscation, forfeiture or withholding of balances must be:

- legally and contractually supportable;
- approved at the appropriate authority level;
- documented with the underlying rationale and evidence; and
- reflected in the customer case record and relevant financial records.

28. MANUAL ADJUSTMENTS, DUAL CONTROLS AND RECONCILIATIONS

28.1 MANUAL ADJUSTMENT PRINCIPLE

Manual adjustments to player balances, withdrawals, refunds, corrections or other financial entries must be exceptional, controlled and documented.

28.2 ADJUSTMENT CONTROLS

All manual adjustments must:

- have a legitimate operational reason;
- be recorded with the date, amount, reason and initiating user;
- be approved in accordance with delegated authority where required; and
- be visible in the relevant ledger, wallet or case history.

28.3 DUAL CONTROL FOR SENSITIVE ACTIONS

Where **Surewin B.V.**'s systems allow, sensitive financial actions should be subject to dual control or maker-checker approval, including:

- high-value balance adjustments;
- exception payments;
- reversals outside standard workflow; and
- closure settlements where balances are disputed.

28.4 RECONCILIATION AND OVERSIGHT

Finance and/or Operations will periodically review:

- manual adjustment logs;
- exception payment activity;
- failed or delayed withdrawal cases;
- PSP settlement discrepancies; and
- unusual patterns in refund or reversal activity.

28.5 MANAGEMENT REVIEW AND ESCALATION

Surewin B.V. maintains a documented Quality Assurance ("QA") Programme to ensure the continued integrity, reliability and compliance of operational processes.

The QA Programme includes:

Daily Monitoring

- gaming platform availability;
- payment gateway availability;
- customer registration;
- withdrawal processing;
- operational incidents;

- system alerts

Change Management

Before implementation of new functionality, appropriate testing will be completed, including:

- functional testing;
- integration testing;
- regression testing;
- user acceptance testing;
- security testing; and
- production verification.

Operational Reviews

Compliance and Operations will periodically review:

- KYC effectiveness;
- transaction monitoring;
- linked transaction detection;
- withdrawal controls;
- fraud controls;
- complaints handling;
- responsible gambling interactions;
- payment reconciliations.

Continuous Improvement

Audit findings, incidents, complaints, compliance reviews and regulatory observations will be analysed to identify opportunities for operational improvement. Corrective actions will be documented, assigned and tracked through to completion.

AML/CFT OPERATIONS

29. AML/CFT GOVERNANCE FRAMEWORK

29.1 PURPOSE

This Part sets out **Surewin B.V.**'s operational AML/CFT framework for identifying, assessing, monitoring, escalating and reporting unusual, suspicious, linked or otherwise high-risk customer activity in connection with the licensed gaming operation.

This Part must be read together with **Surewin B.V.**'s AML/CFT Policy and any applicable legal and regulatory requirements in Curaçao relating to customer due diligence, enhanced due diligence, sanctions compliance, unusual transaction reporting and recordkeeping.

29.2 AML/CFT OBJECTIVES

Surewin B.V.'s AML/CFT operating framework is designed to:

1. prevent the use of **Surewin B.V.**'s services for money laundering, terrorist financing, fraud, sanctions evasion or other criminal misuse;

2. identify high-risk, unusual, suspicious or structured activity at onboarding, during account use and at withdrawal stage;
3. ensure staff understand how and when to escalate internal unusual transaction concerns;
4. ensure the MLRO receives sufficient information to assess whether an internal escalation requires filing of a UTR with the FIU Curaçao; and
5. maintain proper records, audit trails, investigation notes and reporting logs.

29.3 AML/CFT ROLES AND RESPONSIBILITIES

Surewin B.V.'s AML/CFT operational framework is supported by the following roles:

(A) FIRST LINE – OPERATIONAL AND CUSTOMER-FACING STAFF

Customer support, payments, risk, fraud, RG and operations staff are responsible for:

- identifying and escalating unusual, suspicious or inconsistent customer behaviour;
- requesting KYC / EDD information where required by workflow;
- recording accurate case notes and evidence; and
- refraining from tipping off customers.

(B) SECOND LINE – COMPLIANCE / AML OVERSIGHT

Compliance and AML personnel are responsible for:

- supporting escalated reviews;
- ensuring AML controls and procedures are followed;
- assisting with sanctions, PEP, SOF/SOW and high-risk customer reviews; and
- maintaining AML registers and oversight reporting.

(C) THIRD LINE / DECISION AUTHORITY – MLRO

The MLRO is responsible for:

- assessing internal unusual transaction escalations;
- deciding whether a UTR must be submitted to the FIU;
- maintaining the MLRO investigation register;
- directing AML investigations and enhanced monitoring where required; and
- reporting material AML matters to Senior Management and/or the Board.

29.4 NO TIPPING-OFF

No employee may disclose to a customer or third party that:

- the customer has been internally escalated for suspicion;
- a UTR is being considered or has been submitted; or
- law-enforcement, FIU or regulatory engagement has been initiated in relation to the customer, except where disclosure is lawful and expressly authorized.

30. CUSTOMER RISK ASSESSMENT AND ONGOING MONITORING

30.1 RISK-BASED APPROACH

Surewin B.V applies a risk-based approach to AML/CFT monitoring. Customers will be assessed and monitored based on their risk profile, considering factors including:

- jurisdiction of residence, nationality and geolocation indicators;
- occupation, source of funds, source of wealth and expected level of play;
- payment methods used and payment ownership profile;
- transaction size, frequency, velocity and pattern;
- withdrawal behaviour;
- PEP, sanctions or adverse media exposure;
- linked account, fraud or bonus abuse indicators; and
- unusual or inconsistent customer explanations.

30.2 ONGOING MONITORING REQUIREMENT

Customer activity must be monitored throughout the customer lifecycle and not only at onboarding. Monitoring should occur:

- when the customer registers and/or first deposits;
- when cumulative transaction activity reaches internal or legal review thresholds;
- when the customer requests withdrawals;
- when the customer's behaviour changes materially;
- when external alerts, adverse media, sanctions or PEP updates arise; and
- when linked transaction or structuring indicators emerge.

30.3 MONITORING SOURCES

Monitoring may rely on one or more of the following:

- account registration and KYC data;
- gameplay, deposit and withdrawal history;
- payment method usage;
- screening alerts;
- device, IP, geolocation and account-linking indicators;
- chargeback, fraud and bonus abuse signals;
- customer support interactions and explanations; and
- internal investigation findings.

30.4 INTERNAL RISK CATEGORISATION

Surewin B.V may classify customers into internal risk categories such as low, medium or high risk. A customer should be treated as higher risk where one or more material AML indicators exist, including:

- unusual payment behaviour;
- high or rapidly increasing transaction values;
- PEP or sanctions exposure;
- significant source-of-funds uncertainty;
- linked or structured transaction behaviour;
- use of multiple accounts or shared payment instruments;
- high-risk geography exposure; or
- adverse media or criminal intelligence concerns.

31. EDD / SOF / SOW / PEP / SANCTIONS ESCALATION TRIGGERS

31.1 GENERAL PRINCIPLE

Enhanced due diligence and/or AML escalation must be considered where the customer, transaction pattern or supporting information presents heightened ML/TF, sanctions or criminal misuse risk.

31.2 EDD TRIGGERS

EDD may be triggered where one or more of the following apply:

- the customer is identified as a PEP or close associate / family member where relevant;
- the customer is linked to a high-risk or restricted jurisdiction;
- the customer's deposits, withdrawals or transaction pattern are inconsistent with their known profile;
- the customer reaches or exceeds internal high-risk thresholds;
- the customer appears reluctant or unable to provide source of funds / source of wealth information where reasonably required;
- there are linked transaction or structuring indicators;
- there are multiple accounts, payment or beneficial ownership concerns;
- there are serious adverse media or law-enforcement-related concern; or
- there are sanctions alerts or possible true matches.

31.3 SOURCE OF FUNDS / SOURCE OF WEALTH REVIEW

A source of funds or source of wealth review may be required where:

- transaction levels are high or unusual relative to the customer's profile;
- the customer makes large deposits with limited gameplay;
- the customer seeks to withdraw significant sums without a credible explanation of funds;
- the customer's occupation, wealth profile or financial explanation appears inconsistent with their activity; or
- the MLRO, Compliance Officer or senior reviewer directs that SOF / SOW be obtained.

31.4 PEP ESCALATION

Where a customer is identified as a PEP or associated party:

- the customer must be escalated for EDD review;
- appropriate management and/or MLRO approval must be obtained before onboarding or continuation, in accordance with Surewin B.V's AML/CFT Policy; and
- enhanced monitoring must be applied or considered.

31.5 SANCTIONS ESCALATION

Where a sanctions screening alert appears to be a possible true match:

- the account must be escalated immediately to Compliance, AML and/or the MLRO;
- account restrictions may be applied pending review;
- no funds may be released contrary to applicable sanctions obligations or internal freeze instructions; and
- all review steps and conclusions must be documented.

32. SUSPICIOUS ACTIVITY INDICATORS

32.1 PURPOSE

The purpose of this section is to provide operational guidance on indicators that may suggest money laundering, terrorist financing, fraud, sanctions evasion, account misuse or other unusual activity requiring enhanced review or escalation.

The indicators below are not exhaustive. A customer can be escalated even if their conduct does not fit neatly into one example, provided the reviewer has reasonable concern based on the overall facts and context.

32.2 SUSPICIOUS INDICATORS AT ONBOARDING / REGISTRATION STAGE

A customer should be considered for escalation where, during onboarding or early account review, one or more of the following indicators are present:

IDENTITY / KYC CONCERNS

- refusal, delay or avoidance in providing standard KYC documentation without a credible reason;
 - identity or address information that appears inconsistent, altered, forged, unverifiable or otherwise unreliable;
 - information that materially conflicts with other information held by Surewin B.V; or
 - inability or unwillingness to explain the source of funds or the purpose of intended activity where reasonably requested.
-

DUPLICATE / LINKED ACCOUNT INDICATORS

- apparent linkage to another existing or previously closed account through common identifiers such as name, address, device, payment method, email, telephone number or IP;
- connection to an account previously subject to AML, fraud, bonus abuse or regulatory concern; or
- creation of multiple accounts using substantially similar credentials or supporting information.

GEOGRAPHY / SANCTIONS / PROFILE CONCERNS

- registration from a prohibited, restricted or high-risk jurisdiction;
- declared residence conflicting with device, IP, payment or documentation indicators; or
- Sanctions, PEP or adverse media alert arising during onboarding.

BEHAVIOURAL RED FLAGS AT REGISTRATION

- urgency to deposit or withdraw before completing verification;
- unusual testing of account or payment functionality; or
- attempts to avoid standard verification processes or obtain information on how to bypass controls.

32.3 SUSPICIOUS INDICATORS DURING THE ACTIVE RELATIONSHIP

Unusual or suspicious activity during the customer relationship may include:

TRANSACTION BEHAVIOUR

- large or rapidly increasing deposits inconsistent with the customer's known profile;
- multiple deposits followed by little or no gameplay and an early withdrawal request;
- repeated deposits and withdrawals with minimal commercial rationale other than movement of funds;
- multiple failed deposits followed by use of alternative payment instruments or accounts; or
- abrupt shifts in payment behaviour, country of access, spending level or account activity without reasonable explanation.

WITHDRAWAL BEHAVIOUR

- immediate or early withdrawal of funds shortly after deposit without a normal pattern of gaming activity;
 - repeated requests to withdraw un-wagered or barely used funds;
 - withdrawal requests to new, unexplained or non-standard payment routes; or
 - attempts to pressure staff to release funds while verification or review is incomplete.
-

CUSTOMER EXPLANATIONS AND CONDUCT

- implausible, contradictory or evasive explanations for the source of funds, occupation, payment methods or account activity;
- refusal to provide requested information without reasonable justification;
- attempts to manipulate, intimidate or mislead staff during review; or
- unexplained urgency to close the account or withdraw all funds during a review.

32.4 ADDITIONAL HIGH-RISK INDICATORS

Additional indicators that may warrant escalation include:

- reluctance or refusal to provide source of funds / source of wealth information where reasonably requested;
- adverse media suggesting criminal, corruption, sanctions or fraud concerns;
- indications that a payment account, card, wallet or bank account belongs to a third party;
- repeated use of different payment methods with no credible explanation;
- structured low value / high-volume transaction patterns;
- repeated activity clustered around threshold levels; or
- any activity that appears designed to obscure the source, ownership or destination of funds.

33. LINKED TRANSACTIONS / STRUCTURING / AGGREGATION INDICATORS

33.1 PURPOSE

Surewin B.V recognizes that individual transactions may appear routine when viewed in isolation but may indicate heightened AML risk when viewed in aggregate. Staff must therefore consider whether multiple transactions, accounts, payment methods or behaviour are linked, connected or structured in a manner that may conceal the true nature of activity.

33.2 LINKED TRANSACTION INDICATORS

Indicators of linked or connected activity may include:

- multiple deposits or withdrawals carried out within a short timeframe that collectively exceed normal behaviour or review thresholds;
- multiple accounts using the same or similar payment instruments, addresses, devices, IPs or other identifiers;
- repeated use of several payment methods by the same customer without a clear legitimate reason;
- clusters of accounts exhibiting mirrored deposit, withdrawal or gameplay behaviour; or
- a customer splitting deposits or withdrawals into smaller transactions across time or methods.

33.3 STRUCTURING / THRESHOLD AVOIDANCE INDICATORS

The following may indicate structuring or threshold avoidance:

- repeated transactions just below legal or internal review thresholds;
- frequent deposits of similar amounts that appear designed to avoid enhanced review;
- repeated small withdrawals instead of a single larger withdrawal where there is no legitimate explanation; or
- account behaviour changing once a threshold, KYC trigger or review request becomes imminent.

33.4 LOW-VALUE / HIGH-VOLUME PATTERNS

Low-value individual transactions may still be suspicious when repeated at scale. Reviewers must consider whether:

- the cumulative value of deposits or withdrawals over a relevant review period is materially higher than the customer's stated profile would suggest;
- the customer appears to be using volume rather than value to move funds; or
- the pattern is linked to multiple payment methods, accounts or jurisdictions.

33.5 AGGREGATION REQUIREMENT

Where linked or structured activity is suspected, the reviewer must aggregate and assess the relevant transactions over an appropriate period and not limit the review to the latest single transaction only.

34. INTERNAL UNUSUAL TRANSACTION / SUSPICIOUS ACTIVITY ESCALATION

34.1 OBLIGATION TO ESCALATE

Any employee who identifies activity that is unusual, suspicious, inconsistent or otherwise gives rise to AML/CFT concern must escalate the matter internally without delay in accordance with this Manual.

Employees are not required to prove money laundering or criminal conduct before escalating a matter. The purpose of the internal escalation process is to ensure that unusual or suspicious concerns are assessed centrally and consistently by the appropriate control function.

34.2 WHEN TO ESCALATE

Internal escalation must occur where:

- the employee cannot reasonably reconcile the customer's activity with the customer's known profile;
- there are suspicious activity indicators under section 32;
- there are linked transaction or structuring indicators under section 33;
- the customer fails to provide satisfactory KYC / EDD / SOF / SOW information;
- there is a sanctions, PEP, adverse media or law-enforcement-related concern; or
- the employee is otherwise concerned that the account or transaction may involve criminal property, suspicious behaviour or misuse of the platform.

34.3 ESCALATION RECIPIENT

Escalations must be routed in accordance with internal workflow, but where AML/CFT suspicion exists the matter must ultimately reach the MLRO or the AML / Compliance function designated to support the MLRO.

34.4 INFORMATION REQUIRED IN AN INTERNAL ESCALATION

The employee escalating the matter should provide, to the extent available:

- customer name / account ID;
- summary of the activity giving rise to concern;
- dates, amounts, payment methods and relevant transaction history;
- explanation provided by the customer, if any;
- documents reviewed and outstanding information requested;
- details of linked accounts, payment methods or related indicators;
- any immediate action already taken, including holds, restrictions or document requests; and
- the reason the employee considers the matter unusual or suspicious.

34.5 TIMING AND FOLLOW-UP

Internal escalations must be submitted as soon as practicable after the concern is identified. Where further evidence or context is expected shortly, the employee may continue gathering factual information, but must not delay escalation where suspicion already exists.

The employee or relevant team must respond promptly to any follow-up questions from Compliance or the MLRO.

34.6 CUSTOMER COMMUNICATION DURING ESCALATION

During an AML escalation:

- communications to the customer must be limited to lawful operational requests for documents, explanations or standard account status updates; and
- staff must not disclose that the customer has been escalated for suspicion or that a report may be filed.

35. INTERNAL INVESTIGATION PROCEDURE

35.1 PURPOSE

The purpose of an internal AML investigation is to gather and assess sufficient factual information to determine whether the activity can be reasonably explained or whether the matter should remain escalated for MLRO decision-making.

35.2 INVESTIGATION STANDARD

When investigating unusual activity, the reviewer must be thorough, objective and evidence based. The reviewer must not assume that the absence of one obvious red flag means the account is low risk.

35.3 INVESTIGATION STEPS

The reviewer should, where relevant: 1. review the customer's KYC, CDD and EDD history; 2. review deposits, withdrawals, gameplay activity, transaction timing and payment methods; 3. assess whether the customer's current activity is consistent with historic behaviour and known profile; 4. review linked accounts, fraud markers, chargeback history or shared identifiers; 5. review customer communications, explanations and prior requests for documents; 6. review sanctions, PEP or adverse media information where relevant; 7. consider whether the customer's explanation plausibly accounts for the activity; and 8. record all findings, evidence and outstanding questions.

35.4 CASE NOTES

The reviewer must maintain clear notes in the case management system, back-office tool or investigation record, including:

- what triggered the review;
- what information was reviewed;
- what the customer said or provided;
- what conclusions were reached;
- whether the matter was escalated or cleared; and
- who approved the final outcome.

35.5 NO TIPPING-OFF DURING INVESTIGATION

The reviewer may request documents or ask neutral operational questions, but must not inform the customer that the account is under AML suspicion or that a UTR may be filed.

36. REASONABLE GROUNDS FOR SUSPICION / INTERNAL UTR REPORTING

36.1 ESCALATION THRESHOLD

If, after considering the available information, the reviewer cannot reasonably explain the activity or remains concerned that the account, transaction or funds may be linked to criminal conduct, money laundering, terrorist financing, sanctions evasion or other illicit behaviour, the matter must remain escalated to the MLRO for formal consideration.

36.2 INTERNAL REPORTING STANDARD

An internal AML / UTR escalation should answer, as far as possible, the following questions:

WHO?

- Who is the customer?
- Who controls or appears connected to the account?
- Who owns the payment methods or funds involved?

WHAT?

- What activity occurred?
- What is unusual, inconsistent or suspicious about it?
- What transactions, documents or behaviour are relevant?

WHEN?

- When did the activity occur?
- Over what period has the behaviour developed?
- Are there recurring or linked events?

WHY?

- Why does the reviewer consider the activity suspicious or unusual?
- Why is the customer explanation inadequate, inconsistent or implausible?
- Why does the reviewer believe escalation is required?

36.3 REVIEWER ROLE VS MLRO ROLE

The operational reviewer's role is to identify and articulate the concern and provide relevant facts. The reviewer is not required to determine whether a UTR will be filed; that decision sits with the MLRO.

37. FIU CURAÇAO GOAML REPORTING PROCEDURE

37.1 PURPOSE

Surewin B.V will maintain operational capability to submit unusual transaction reports to the FIU Curaçao via the goAML platform where the MLRO determines that reporting is required.

37.2 REPORTING AUTHORITY

Only the MLRO or another specifically authorized person acting under the MLRO's authority may approve or submit a UTR to the FIU on behalf of **Surewin B.V**.

37.3 GOAML ACCESS AND REGISTRATION

Surewin B.V confirms that:

- it is registered with the FIU / goAML as required;
- the MLRO and any authorized backup users have access to the reporting platform; and
- access credentials are securely controlled and updated where personnel change.

37.4 SUBMISSION PROCEDURE

Where the MLRO determines that a UTR must be filed:

1. the relevant facts, documents and transaction details must be collated;
2. the MLRO will prepare or approve the report content;
3. the UTR will be submitted via goAML in accordance with applicable FIU requirements; and
4. the date of submission, reference details and any subsequent FIU correspondence must be recorded in the AML reporting log.

37.5 SUPPORTING EVIDENCE

Surewin B.V will retain supporting evidence relating to each UTR decision, including:

- internal escalation records;
- investigation notes;
- relevant customer data and transaction history;
- copies of information submitted to the FIU; and
- any FIU follow-up correspondence or requests.

37.6 CONFIDENTIALITY

All UTR-related information must be handled on a strict need-to-know basis and stored securely.

38. MLRO INVESTIGATION REGISTER

38.1 PURPOSE

The MLRO will maintain a register of unusual internal transaction / suspicious activity escalations received and investigated. The register is intended to provide:

- an auditable record of AML concerns raised internally;
- evidence of the MLRO's review and decision-making; and
- a basis for reporting, quality assurance, training and regulatory inspection.

38.2 MINIMUM REGISTER FIELDS

The MLRO investigation register should, at minimum, record:

- internal case reference;
- date escalated;
- customer ID / name;
- reason for escalation / trigger summary;
- key transaction details and value where relevant;
- reviewer / escalator;
- investigation steps taken;
- MLRO decision;

- whether a UTR was filed;
- date of UTR filing where applicable; and
- final account outcome, restrictions, closure or monitoring actions.

38.3 REGISTERING NON-REPORTABLE CASES

The register must include not only cases resulting in a UTR, but also cases reviewed and closed without external reporting, provided they involved a meaningful AML escalation. This supports auditability and demonstrates that **Surewin B.V** actively reviews unusual activity even where the legal reporting threshold is not met.

38.4 PERIODIC REVIEW USE

The register may be used to identify:

- repeated customer typologies;
- training needs;
- recurring payment, jurisdiction or source-of-funds risks; and
- process weaknesses or delays in escalation.

39. AML REGISTERS, RECORDKEEPING, TRAINING AND AUDIT

39.1 AML REGISTER SUITE

Surewin B.V will maintain, either within the MLRO register or as separate logs, the following AML-related records where applicable:

- internal suspicious activity / unusual transaction escalation log;
- MLRO investigation register;
- UTR / goAML reporting log;
- sanctions / PEP escalation log;
- EDD / high-risk customer register;
- AML training register;
- AML audit / QA findings tracker; and
- law-enforcement / FIU request log where applicable.

39.2 RECORDKEEPING

All AML records must:

- be stored securely and access-controlled;
- be sufficiently detailed to reconstruct the review and decision process;
- be retained in accordance with **Surewin B.V**'s AML/CFT Policy, record retention schedule and applicable law; and
- be available for internal review and regulatory inspection where lawfully required.

39.3 AML TRAINING

Relevant staff must receive AML/CFT training appropriate to their role, including:

- suspicious activity indicators;
- internal escalation requirements;
- tipping-off restrictions;
- source of funds / EDD triggers;
- linked transaction and structuring indicators; and
- MLRO reporting lines and use of internal registers.

39.4 AUDIT AND QUALITY ASSURANCE

Surewin B.V will periodically review the effectiveness of its AML operational controls, including:

- quality of internal escalations;
- timeliness of investigation and MLRO review;
- adequacy of KYC / EDD evidence;
- appropriateness of UTR decision-making records; and
- effectiveness of linked transaction detection and threshold aggregation controls.

40. RESPONSIBLE GAMBLING GOVERNANCE

40.1 PURPOSE

This Part sets out **Surewin B.V**'s operational framework for responsible gambling ("RG"), including player protection controls, age verification, identification of vulnerable or at-risk customers, customer interventions, self-exclusion and cooling-off controls, operator-imposed restrictions and RG recordkeeping.

40.2 RESPONSIBLE GAMBLING OBJECTIVE

Surewin B.V will conduct its gaming operations in a manner that promotes safer gambling, protects minors and vulnerable persons and provides customers with access to information, tools and interventions designed to reduce gambling-related harm.

40.3 GOVERNANCE AND OWNERSHIP

Surewin B.V will maintain a designated Responsible Gambling Officer or equivalent function holder responsible for oversight of **Surewin B.V**'s RG framework.

The Responsible Gambling Officer will have authority to:

- oversee implementation of the Responsible Gambling Policy and the operational controls in this Manual;
- review and direct interventions in high-risk or vulnerable customer cases;
- oversee self-exclusion, cooling-off and operator-imposed restriction processes;
- liaise with customer support, risk, compliance and senior management on serious RG matters;

- ensure RG records, logs and escalation registers are maintained; and
- support reporting and periodic review of RG trends, incidents and control effectiveness.

40.4 SHARED RESPONSIBILITY ACROSS THE BUSINESS

Responsible gambling is not the responsibility of the Responsible Gambling Officer alone. Customer support, payments, fraud, compliance, risk and operational staff must identify and escalate indicators of customer harm, distress, loss of control or vulnerability in accordance with this Manual and the Responsible Gambling Policy.

40.5 RELATIONSHIP WITH THE RESPONSIBLE GAMBLING POLICY

This Part must be read together with **Surewin B.V.**'s Responsible Gambling Policy, customer-facing responsible gambling terms and any safer gambling procedures, tools or product controls maintained by **Surewin B.V.**

41. AGE VERIFICATION AND UNDERAGE GAMBLING CONTROLS

41.1 NO MINOR PLAY

Surewin B.V. will not knowingly permit any person below the legal minimum age to register, deposit, gamble or withdraw through the platform.

41.2 AGE VERIFICATION CONTROLS

Surewin B.V. will apply age verification and related eligibility controls through:

- collection of date of birth and identity information at registration;
- KYC verification processes and document review;
- account review where date of birth, identity or account ownership is unclear, inconsistent or disputed; and
- account restriction where age cannot be satisfactorily verified.

41.3 UNDERAGE ESCALATION PROCEDURE

If **Surewin B.V.** becomes aware or reasonably suspects that an account may belong to a minor: 1. the account must be restricted immediately; 2. the matter must be escalated to the Responsible Gambling Officer and Compliance without delay; 3. further verification must be obtained where appropriate; 4. the account must remain blocked or restricted until the matter is resolved; and 5. if underage gambling is confirmed, **Surewin B.V.** will take appropriate remedial action in accordance with law, policy, the Terms and Conditions and internal approval requirements.

41.4 RECORDKEEPING

All underage gambling concerns, investigations, restrictions and outcomes must be recorded in the relevant RG case notes and, where material, in the RG incident or escalation register.

42. VULNERABLE CUSTOMER IDENTIFICATION AND RISK CLASSIFICATION

42.1 PURPOSE

Surewin B.V will maintain procedures to identify customers who may be at risk of gambling-related harm or who otherwise display vulnerability indicators requiring intervention.

42.2 SOURCES OF RG RISK INDICATORS

RG concerns may arise from one or more of the following:

- transaction patterns or repeated escalating deposits;
- repeated failed deposit attempts;
- extended, repetitive or unusually intensive gameplay;
- repeated requests to reverse withdrawals or release held funds urgently;
- customer statements indicating distress, financial pressure, loss of control or inability to stop gambling;
- repeated requests to increase, remove or bypass gambling limits;
- self-exclusion / reactivation cycles or repeated short cooling-off periods;
- complaints or contacts from family members or third parties raising welfare concerns; or
- staff observations from support interactions or case reviews.

42.3 RISK-BASED RG CLASSIFICATION

Surewin B.V may categorize customers into internal RG risk levels such as low, medium, high or critical risk. Indicators relevant to risk classification may include:

- frequency, intensity and affordability indicators associated with the customer's gambling behaviour;
- evidence of chasing losses or gambling beyond the customer's apparent means;
- signs of financial harm, distress, borrowing to gamble or gambling with essential living funds;
- emotional, distressed, erratic or self-disclosing customer communications;
- inability to stop, repeated failed attempts to control spending or repeated requests to override limits; and
- persistent attempts to remove, bypass or undermine safer gambling controls.

42.4 ESCALATION REQUIREMENT

Where staff identify a customer who may be vulnerable or at risk, the case must be escalated promptly to the relevant RG workflow in accordance with Surewin B.V's intervention matrix and approval routes.

42.5 INTERACTION WITH AML, FRAUD AND COMPLAINTS

Where an RG concern overlaps with AML, fraud, payment disputes or a customer complaint, the relevant control functions must coordinate their review. A serious RG concern must not be disregarded merely because another operational issue is also under investigation.

43. RG INTERVENTIONS, CUSTOMER CONTACT AND SAFER GAMBLING ACTIONS

43.1 PRINCIPLE

Where RG risk indicators arise, **Surewin B.V** will act proportionately to the level of risk and the customer's circumstances. Action may range from monitoring and safer gambling messaging to direct intervention, account restriction or exclusion.

43.2 TYPES OF RG ACTION

Depending on the risk level, **Surewin B.V** may take one or more of the following actions:

- enhanced monitoring of the account;
- safer gambling prompts, information or messaging;
- encouragement or requirement to use deposit, loss, wagering or session limits where available;
- discussion of cooling-off or self-exclusion options;
- direct contact by RG-trained staff;
- suppression of promotional communications; and
- operator-imposed restrictions, account suspension or closure in severe cases.

43.3 DIRECT CUSTOMER CONTACT

Where **Surewin B.V** determines that direct contact is appropriate, the interaction should:

- be conducted by RG-trained staff or the Responsible Gambling Officer;
- be professional, supportive and non-judgmental;
- encourage use of safer gambling tools and support resources;
- avoid encouraging continued play or minimizing the seriousness of the concern; and
- be documented in the RG interaction record.

43.4 PROMOTIONAL SUPPRESSION

Customers identified as medium, high or critical RG risk may be removed from promotional campaigns or excluded from marketing contact where required by policy, operational workflow or case assessment.

43.5 FOLLOW-UP AND ONGOING MONITORING

Where an intervention has been carried out, **Surewin B.V** may apply follow-up monitoring, repeated contact or further restrictions if the customer's behaviour continues to present concern.

44. LIMITS, COOLING-OFF, SELF-EXCLUSION AND OPERATOR-IMPOSED RESTRICTIONS

44.1 CUSTOMER PROTECTION TOOLS

Surewin B.V will provide or otherwise support access to customer protection tools such as:

- deposit limits;
- loss, wagering or session limits where available;
- time reminders or session management tools where available;
- cooling-off periods; and
- self-exclusion.

44.2 COOLING-OFF REQUESTS

Where a customer requests a cooling-off period, the request must be processed promptly, recorded in the relevant register and applied to the account in accordance with the Responsible Gambling Policy and platform capability.

44.3 SELF-EXCLUSION REQUESTS

Self-exclusion requests must be actioned promptly and without unnecessary barriers. Once applied:

- the account must be restricted in accordance with the exclusion settings;
- promotional contact must be suppressed where required;
- the self-exclusion must be recorded in the self-exclusion register and case notes; and
- reactivation must follow **Surewin B.V**'s reactivation rules and approval process.

44.4 OPERATOR-IMPOSED RESTRICTIONS OR EXCLUSIONS

Where **Surewin B.V** determines that a customer presents a serious risk of harm, **Surewin B.V** may impose restrictions, suspend the account or exclude the customer in accordance with the Approval Matrix, the Responsible Gambling Policy and the RG intervention framework.

44.5 REACTIVATION CONTROLS

Where reactivation is permitted after cooling-off or self-exclusion, **Surewin B.V** may require:

- expiry of the minimum exclusion period;
- a customer request to reactivate;
- RG review before reactivation; and

- application of limits, monitoring or other safeguards upon return.

45. RG RECORDS, ESCALATIONS AND REPORTING

45.1 RG RECORDS

Surewin B.V will maintain sufficient records of RG reviews, interventions and exclusions, including:

- risk indicators observed;
- risk level assigned;
- actions taken;
- customer contacts made;
- self-exclusion and cooling-off records;
- reactivation decisions and conditions; and
- operator-imposed restrictions and the rationale for them.

45.2 RG ESCALATION

Material RG concerns must be escalated to the Responsible Gambling Officer and, where appropriate, to Compliance and Senior Management, including:

- underage gambling concerns;
- serious vulnerability or financial harm indicators;
- repeated failed interventions;
- customer complaints alleging RG failures; and
- cases involving legal, regulatory or reputational risk.

45.3 RG REPORTING

Surewin B.V will maintain periodic reporting on:

- self-exclusion volumes;
- cooling-off requests;
- high-risk interventions;
- operator-imposed exclusions or restrictions;
- recurring RG complaint themes; and
- material RG incidents or control weaknesses.

46. CUSTOMER SUPPORT OPERATING MODEL WEBSITE AND PLAYER INTERFACE CONTROLS - COMPLAINTS AND ADR

Surewin B.V will ensure that all customer-facing websites and applications display accurate, transparent and up-to-date information.

Where applicable, the gaming website will display:

- Company name;
- Curaçao Gaming Authority License information;
- Terms and Conditions;

- Privacy Notice;
- Responsible Gambling information;
- Self-Exclusion functionality;
- Deposit, Loss wager Limit tools;
- Minimum age requirement (18+);
- Complaint submission process;
- Approved Alternative Dispute Resolution (ADR) provider details;
- Customer Support contact information;
- Accepted payment methods; and
- Promotional terms and conditions.

Customer-facing information will be reviewed periodically to ensure continued accuracy and compliance.

46.1 SUPPORT FUNCTION

Surewin B.V will maintain a customer support function to receive and respond to customer queries, complaints, operational requests and escalation matters relating to the licensed business.

46.2 SUPPORT RESPONSIBILITIES

Customer support staff are responsible for:

- responding to routine customer queries and service requests;
- escalating KYC, withdrawal, RG, AML, fraud and complaint matter to the relevant teams;
- recording customer interactions and operational notes accurately and promptly; and
- ensuring customer-facing communications remain consistent with this Manual, the Terms and Conditions and **Surewin B.V**'s policies.

46.3 SUPPORT LIMITATIONS

Customer support staff may not override:

- AML or sanctions restrictions;
- MLRO reporting decisions or AML escalation outcomes;
- RG exclusions or restrictions;
- payment or withdrawal controls outside delegated authority; or
- complaint outcomes that require management, compliance or legal approval.

46.4 RECORDKEEPING

Customer support interactions relevant to KYC, AML, RG, complaints, payment disputes, fraud concerns or operational escalations must be recorded in the relevant ticketing or case management system.

47. PLAYER INTERACTIONS, COMPLAINTS AND DISPUTES

47.1 COMPLAINT DEFINITION

For the purposes of this Manual, a complaint is an expression of dissatisfaction by a customer concerning **Surewin B.V.**'s products, services, account handling, payments, responsible gambling actions, technical issues or conduct of staff where the customer seeks a response, remedy or resolution.

47.2 COMPLAINT INTAKE CHANNELS

Complaints may be received through:

- email;
- support tickets;
- live chat;
- other approved customer contact channels; or
- escalation from support or management.

47.3 COMPLAINT LOGGING

All complaints must be logged in **Surewin B.V.**'s complaints register or complaint handling system with sufficient detail to identify:

- the customer and account concerned;
- the date received;
- the subject matter and category of complaint;
- the assigned owner or handler;
- the current status; and
- the outcome and closure date.

47.4 COMPLAINT CATEGORIES

Complaints may include, by way of example:

- withdrawal or payment disputes;
- KYC / verification complaints;
- bonus or promotion disputes;
- game or technical complaints;
- RG complaints;
- account restriction or closure complaints;
- customer service complaints; and
- data or privacy-related complaints.

48. COMPLAINT INVESTIGATION AND INTERNAL ESCALATION

48.1 FAIR HANDLING PRINCIPLE

Complaints must be handled fairly, promptly, consistently and with appropriate regard to customer protection, contractual terms, regulatory obligations and internal controls.

48.2 COMPLAINT INVESTIGATION

The complaint handler or designated owner must:

- review the complaint and relevant account history;
- obtain supporting evidence, transaction history, support logs or policy references as needed;
- liaise with payments, fraud, RG, compliance or technical teams where relevant; and
- prepare a clear outcome with reasons.

48.3 MANDATORY ESCALATION

A complaint must be escalated where it involves:

- high-value withdrawals, confiscations or disputed balances;
- AML, sanctions or fraud allegations;
- self-exclusion, underage or serious RG concerns;
- potential legal, regulatory or reputational risk;
- repeated or systemic operational issues; or
- a request for compensation or remedy outside the handler's delegated authority.

48.4 COMPLAINT OUTCOME

The complaint outcome should:

- address the issues raised;
- explain Surewin B.V's decision and the supporting rationale;
- set out any corrective action, goodwill gesture or further escalation route where applicable; and
- be recorded in the complaint file and complaints register.

49. ADR AND EXTERNAL DISPUTE RESOLUTION

49.1 ADR PROVIDER

Surewin B.V's appointed ADR provider is **CADRE**.

49.2 REFERRAL TO ADR

Where a complaint remains unresolved after completion of Surewin B.V's internal complaints process, the customer may be referred to ADR in accordance with the Complaints Handling Policy and the rules of the appointed ADR provider.

49.3 ADR CASE HANDLING

Where a complaint is referred to ADR:

- the case must be logged in the ADR escalation log;
- the Complaints Owner and Compliance Officer must be notified;

- a case pack must be prepared containing the relevant complaint history, evidence, transaction information and internal decision rationale; and
- any AML, RG or fraud-sensitive information must be reviewed before disclosure to ensure lawful and appropriate sharing.

49.4 ADR OUTCOME MANAGEMENT

Surewin B.V will:

- cooperate in good faith with the ADR process;
- review and implement any customer remediation or internal corrective action required by the outcome;
- update the complaints and ADR registers accordingly; and
- report material ADR outcomes or trends to Senior Management.

50. COMPLAINTS REGISTERS, REPORTING AND GOVERNANCE

50.1 COMPLAINTS REGISTER

Surewin B.V will maintain complaints register recording, at minimum:

- complaint reference;
- customer account details;
- date received;
- category;
- assigned owner;
- status;
- outcome and closure date; and
- whether the complaint escalated to ADR or management review.

50.2 COMPLAINTS REPORTING

Periodic complaints reporting should include:

- number of complaints by category;
- unresolved or aged complaints;
- average response and resolution times;
- repeat complaint themes;
- complaints escalated to ADR; and
- complaints with RG, AML, fraud or payment relevance.

50.3 GOVERNANCE REVIEW

Material complaint themes, systemic failures, ADR outcomes and high-severity disputes must be escalated to Compliance and Senior Management and included in periodic governance reporting.

INFORMATION SECURITY, ACCESS, CHANGE AND INCIDENT MANAGEMENT

51. INFORMATION SECURITY GOVERNANCE

51.1 SECURITY PRINCIPLE

Surewin B.V will maintain an information security framework appropriate to the nature, scale and risk of its licensed operation in order to protect:

BO – Role Based Access

- customer data;
- payment information;
- account credentials;
- gaming systems and operational records; and
- regulatory reporting records, investigation files and internal case records.

51.2 SECURITY OVERSIGHT

Surewin B.V will designate an IT / Security Owner or equivalent responsible person to oversee information security controls, supported where relevant by outsourced service providers and internal control functions. **Surewin B.V** has designated Cornel Storm as the CTO (IT Security owner)

51.3 RELATIONSHIP WITH SECURITY POLICY

This Part must be read together with **Surewin B.V**'s Information Security Policy and any applicable access control, incident response, vendor management and business continuity procedures.
L:\Documentation\Wiki's\Security\Policies\Blanks\ Information Security Policy.docx

52. ACCESS CONTROL, USER RIGHTS AND PRIVILEGED ACCESS

52.1 ACCESS RESTRICTION PRINCIPLE

Access to systems, records and customer data must be granted on a role-based, least privileged basis and only to personnel with a legitimate business need.

52.2 USER ACCESS CONTROLS

Surewin B.V will maintain controls over:

- new user access requests and approvals;
- changes to user permissions;
- removal of access on role change or termination;
- periodic access reviews; and
- privileged or administrator access.

52.3 SENSITIVE SYSTEMS

Particular care must be taken with access to:

- player account management systems;
- withdrawal and payment tools;
- AML, RG and complaint case records;
- KYC document repositories;
- goAML / FIU reporting access;
- security logs and configuration settings; and
- any system capable of making manual financial or account-status changes.

52.4 SHARED CREDENTIALS

Shared credentials should be avoided wherever possible. Where unavoidable, their use must be tightly controlled, documented and subject to enhanced oversight.

53. CHANGE MANAGEMENT, SYSTEM OVERRIDES AND OUTSOURCED DEVELOPMENT

53.1 CHANGE MANAGEMENT PRINCIPLE

Material changes to systems, payment flows, RG controls, withdrawal rules, KYC workflows, customer-facing terms or other processes affecting the licensed operation must be assessed, approved, tested and documented before implementation.

53.2 CHANGE APPROVAL

Change requests should identify:

- the proposed change;
- the reason for the change;
- the systems, controls or customer groups affected;
- the risks and dependencies;
- the testing and rollback arrangements; and
- the approver or approvers.

53.3 SYSTEM OVERRIDES AND MANUAL WORKAROUNDS

Where a system override or manual workaround is required:

- the reason must be documented;
- approval must be obtained in accordance with delegated authority;
- the override must be limited to what is necessary; and
- the incident or workaround must be reviewed for control impact.

53.4 OUTSOURCED DEVELOPMENT / SUPPLIER CHANGES

Where third-party suppliers make changes affecting the licensed operation, Surewin B.V will ensure there is sufficient visibility over:

- the nature of the change;
- the expected impact;
- testing and implementation timelines; and
- contingency arrangements if the change fails or causes disruption.

54. INCIDENT MANAGEMENT AND BREACH ESCALATION

54.1 INCIDENT DEFINITION

An incident is any event that disrupts, threatens or adversely affects the integrity, security, availability, compliance or proper operation of the licensed business.

54.2 INCIDENT CATEGORIES

Incidents may include:

- AML or sanctions control failures;
- RG failures or self-exclusion failures;
- erroneous withdrawals, wallet issues or payment incidents;
- fraud events or payment abuse incidents;
- data breaches or security incidents;
- platform outages or game malfunctions;
- supplier failures; and
- complaint handling failures causing material customer impact.

54.3 INCIDENT RESPONSE

Where an incident occurs, the Company will:

- identify and contain the issue;
- preserve evidence where relevant;
- assess customer, regulatory, financial and operational impact;
- escalate to the appropriate owner and control functions; and
- implement remedial action and monitor resolution.

54.4 SEVERITY AND ESCALATION

Incidents will be assessed by severity. Material or critical incidents must be escalated promptly to Senior Management and, where relevant, to Compliance, the MLRO, the Responsible Gambling Officer, IT / Security and the Board.

54.5 INCIDENT LOGGING

All material incidents must be recorded in the incident log or equivalent register, including:

- date and time;
- description of incident;
- systems or customers affected;
- owner;
- immediate action taken; and
- remediation status and, where available, root cause information.
- These are done via It Helpdesk, ES Jira, Security, Joes Slack Channel.

55. REGULATORY, FIU AND LAW-ENFORCEMENT COOPERATION

55.1 COOPERATION OBLIGATION

Surewin B.V will cooperate with lawful requests from:

- the Curaçao Gaming Authority;
- the FIU Curaçao;
- law-enforcement agencies;
- courts or other competent authorities; and
- ADR bodies where appropriate.

55.2 HANDLING OF REQUESTS

Requests for customer information, account data, transaction records or operational records must be routed to the appropriate internal owner, which may include:

- Compliance;
- the MLRO;
- Legal / Senior Management; and
- IT / Security where technical extraction is required.

55.3 CONFIDENTIALITY AND RECORDKEEPING

All external requests and responses must be handled confidentially and logged in the relevant register, including the request date, requesting authority, owner, response deadline and date completed.

56. BUSINESS CONTINUITY AND DISASTER RECOVERY

56.1 CONTINUITY PRINCIPLE

Surewin B.V will maintain arrangements reasonably designed to support continuity of critical licensed operations during outages, incidents, supplier failures or other disruptions.

56.2 CRITICAL PROCESSES

Continuity planning should cover, at minimum:

- access to player account and transaction records;
- handling of withdrawals and payment exceptions;
- customer support continuity;
- AML, RG and complaint escalation capability;
- security incident response; and
- communication with key suppliers and internal stakeholders.

56.3 CONTINGENCY PLANNING

Surewin B.V will maintain contingency arrangements or documented fallback processes for critical supplier or system failure, including escalation contacts and decision-making authority.

57. DIGITAL RECORDS AND DATA MANAGEMENT

Surewin B.V maintains complete and accurate electronic records relating to customer activity and operational controls.

Digital records include:

- customer registration records;
- identity verification documentation;
- KYC records;
- Enhanced Due Diligence records;
- Source of Funds and Source of Wealth documentation;
- deposits and withdrawals;
- gaming transactions;
- payment records;
- bonus activity;
- responsible gambling interactions;
- customer complaints;
- linked transaction investigations;
- fraud investigations;
- MLRO investigations;
- Unusual Transaction Reports;
- audit logs;
- employee training records;
- Board approvals and governance records.

Access to operational records will be restricted to authorised personnel through role-based access controls.

Records will be protected through appropriate technical and organisational security measures, retained in accordance with **Surewin B.V**'s Record Retention Schedule and applicable legal requirements, and made available to the Curaçao Gaming Authority upon lawful request.

58. REGULATORY INCIDENT NOTIFICATION

58.1 REPORTABLE INCIDENTS

Surewin B.V will identify, investigate, document and report all material operational, security and gaming incidents that may impact the integrity, reliability, transparency or availability of its licensed gaming operations.

At a minimum, reportable incidents include:

- Gaming security breaches that have, or may have, compromised player personal information, confidential gaming information or other critical operational data;
- Failure, loss of, or damage to equipment, systems or software that has resulted in, or may result in, the interruption, degradation or loss of any part of **Surewin B.V**'s Remote Gaming operations;
- Gaming-related fraud, attempted fraud, cybercrime or other criminal activity involving players, employees, suppliers or third parties connected with the licensed operation;
- Any other event, circumstance or behaviour that may pose a serious threat to the responsible, reliable, transparent or verifiable operation of **Surewin B.V**'s gaming activities or may undermine public confidence in **Surewin B.V**'s licensed operations.

58.2 REGULATORY NOTIFICATION

Where a reportable incident is identified, **Surewin B.V** will notify the Curaçao Gaming Authority (CGA) by submitting an Incident Report as soon as reasonably practicable and, in all cases, within twenty-four (24) hours of becoming aware of the incident, in accordance with Article 5.10 of the National Ordinance on Games of Chance (LOK).

58.3 INCIDENT MANAGEMENT

The Incident Report will include, where applicable:

- the date and time the incident occurred and was detected;
- a description of the incident and its impact;
- affected systems, games, services or player data;
- immediate containment and mitigation measures implemented;
- corrective actions and recovery activities;
- the current operational status; and
- any additional information requested by the CGA.

All reportable incidents will be recorded in **Surewin B.V**'s Incident Register and retained in accordance with **Surewin B.V**'s record retention requirements. Following closure of the incident, a root cause analysis will be completed, and any corrective or preventive actions will be implemented and monitored to completion.

59. CHANGES TO THIS OPERATIONS MANUAL

Please note that this Operations Manual may change from time to time.
