

Operational Manual

Company

AG Group B.V.

Document Version

1.0

Effective Date

July 2026

Document Owner

Director

Document Status

Approved

This document describes the operational procedures and compliance framework adopted by AG Group B.V. as a Curaçao licensed operator.

	2
1. Company Information	8
2. Organisational Structure	8
2.1 Overview	8
2.2 Organisation Structure	8
2.3 Roles and Responsibilities	8
Director	8
Compliance	9
Operations	9
Finance	9
Customer Support	10
IT / Technical	10
2.4 Segregation of Duties	11
2.5 Reporting Lines	11
3. Business Activities	11
3.1 Business Overview	11
3.2 Services Provided	11
3.3 Operational Markets	12
3.4 Online Gaming Operations	12
3.5 Player Account Management	12
3.6 Payment Management	13
3.7 Responsible Gaming	13
3.8 AML/CFT Compliance	14
4. Governance and Responsibilities	14
4.1 Governance Framework	14
4.2 Roles and Responsibilities	14
4.3 Decision-Making Authority	15
4.4 Segregation of Duties	16
4.5 Internal Reporting	16
4.6 Policy Review	17
5. Operational Procedures	17
5.1 Daily Operations	17
5.2 Customer Registration	17
5.3 Player Login and Account Access	18
5.4 Deposit Procedures	18
5.5 Gaming Operations	19
5.6 Withdrawal Procedures	19
5.7 Customer Support	19
5.8 Account Suspension and Closure	20
5.9 Operational Monitoring	20
5.10 Incident Escalation	20

5.11 Daily Operational Checklist	21
5.12 Operational Workflow	21
6. Customer Registration and KYC	22
6.1 Customer Registration	22
6.2 Identity Verification (KYC)	23
6.3 Enhanced Due Diligence (EDD)	23
6.4 Ongoing Customer Monitoring	24
6.5 Record Retention	24
6.6 Registration and KYC Workflow	25
7. AML/CFT Compliance	25
7.1 Overview	25
7.2 Risk-Based Approach	26
7.3 Customer Due Diligence (CDD)	26
7.4 Enhanced Due Diligence (EDD)	26
7.5 Transaction Monitoring	27
7.6 Sanctions and PEP Screening	27
7.7 Suspicious Activity Reporting	28
7.8 Record Retention	28
7.9 Staff Training	28
7.10 AML/CFT Workflow	29
7.11 Reference Documents	29
8. Responsible Gaming	29
8.1 Purpose	29
8.2 Responsible Gaming Principles	30
8.3 Age Verification	30
8.4 Responsible Gaming Tools	30
8.5 Self-Exclusion	31
8.6 Customer Support	31
8.7 Staff Awareness	31
8.8 Monitoring and Review	32
8.9 Reference Documents	32
8.10 Responsible Gaming Workflow	32
9. Player Complaints Handling	33
9.1 Purpose	33
9.2 Scope	33
9.3 Complaint Submission	34
9.4 Complaint Investigation	34
9.5 Complaint Resolution	34
9.6 Escalation	35
9.7 Record Retention	35

9.8 Monitoring and Continuous Improvement	35
9.9 Reference Documents	36
9.10 Complaint Handling Workflow	36
10. Payment Processing and Fund Management	36
10.1 Purpose	36
10.2 Accepted Payment Methods	36
10.3 Deposit Procedures	37
10.4 Withdrawal Procedures	37
10.5 Payment Monitoring	38
10.6 Customer Funds	38
10.7 Reconciliation	38
10.8 Payment Security	39
10.9 Record Retention	39
10.10 Reference Documents	40
10.11 Payment Processing Workflow	40
11. Personal Data Protection	40
11.1 Purpose	40
11.2 Collection of Personal Data	41
11.3 Use of Personal Data	41
11.4 Data Security	42
11.5 Data Retention	42
11.6 Data Sharing	42
11.7 Data Subject Rights	43
11.8 Confidentiality	43
11.9 Reference Documents	43
11.10 Personal Data Protection Workflow	44
12. Information Security	44
12.1 Purpose	44
12.2 Information Security Objectives	44
12.3 Access Control	45
12.4 Authentication and Password Security	45
12.5 Network and System Security	45
12.6 Data Security	46
12.7 Logging and Monitoring	46
12.8 Security Incident Management	47
12.9 Backup and Recovery	47
12.10 Security Awareness	47
12.11 Reference Documents	48
12.12 Information Security Workflow	48
13. Business Continuity	48

13.1 Purpose	48
13.2 Scope	49
13.3 Business Continuity Objectives	49
13.4 Business Continuity Planning	49
13.5 Roles and Responsibilities	50
13.6 Communication During Disruptions	51
13.7 Periodic Review and Testing	51
13.8 Documentation and Record Keeping	51
13.9 Reference Documents	52
13.10 Business Continuity Workflow	52
14. Disaster Recovery	52
14.1 Purpose	52
14.2 Scope	53
14.3 Disaster Recovery Objectives	53
14.4 Disaster Recovery Events	53
14.5 Backup Procedures	54
14.6 Recovery Procedures	54
14.7 Recovery Testing	55
14.8 Roles and Responsibilities	55
14.9 Documentation and Record Keeping	56
14.10 Reference Documents	56
14.11 Disaster Recovery Workflow	56
14.12 Continuous Improvement	57
15. Record Retention	57
15.1 Purpose	57
15.2 Scope	57
15.3 Record Retention Period	58
15.4 Record Protection	59
15.5 Access to Records	59
15.6 Record Disposal	59
15.7 Monitoring and Review	60
15.8 Reference Documents	60
15.9 Record Retention Workflow	60
16. Regulatory Reporting	61
16.1 Purpose	61
16.2 Regulatory Reporting Responsibilities	61
16.3 Regulatory Notifications	61
16.4 Regulatory Inspections and Audits	62
16.5 Record Keeping	62
16.6 Internal Review	62

16.7 Continuous Compliance	63
16.8 Reference Documents	63
16.9 Regulatory Reporting Workflow	63
17. Internal Controls	64
17.1 Purpose	64
17.2 Internal Control Objectives	64
17.3 Segregation of Duties	64
17.4 Approval Controls	65
17.5 Operational Monitoring	65
17.6 Risk Assessment	65
17.7 Internal Reviews	66
17.8 Corrective Actions	66
17.9 Documentation and Record Keeping	67
17.10 Reference Documents	67
17.11 Internal Control Workflow	67
18. Incident Management	68
18.1 Purpose	68
18.2 Scope	68
18.3 Incident Identification	68
18.4 Incident Classification	69
18.5 Incident Response	69
18.6 Escalation Procedures	70
18.7 Incident Documentation	70
18.8 Post-Incident Review	70
18.9 Continuous Improvement	71
18.10 Reference Documents	71
18.11 Incident Management Workflow	71
19. Third-Party Service Providers	72
19.1 Purpose	72
19.2 Scope	72
19.3 Selection and Due Diligence	73
19.4 Contractual Arrangements	73
19.5 Ongoing Monitoring	73
19.6 Information Security	74
19.7 Regulatory Compliance	74
19.8 Termination of Third-Party Services	74
19.9 Reference Documents	75
19.10 Third-Party Management Workflow	75
20. Document Control	75
20.1 Purpose	75

20.2 Scope	76
20.3 Document Ownership	76
20.4 Document Review	76
20.5 Version Control	77
20.6 Document Approval	77
20.7 Document Distribution	77
20.8 Record Retention	78
20.9 Reference Documents	78
20.10 Document Control Workflow	78
21. Risk Management	78
21.1 Purpose	78
21.2 Risk Management Framework	79
21.3 Risk Identification	79
21.4 Risk Assessment	80
21.5 Risk Mitigation	80
21.6 Risk Monitoring	80
21.7 Management Review	81
21.8 Continuous Improvement	81
21.9 Reference Documents	82
21.10 Risk Management Workflow	82
22. Training and Staff Awareness	82
22.1 Purpose	82
22.2 Scope	82
22.3 Induction Training	83
22.4 Compliance Training	83
22.5 AML/CFT Training	83
22.6 Responsible Gaming Training	84
22.7 Information Security and Data Protection Training	84
22.8 Refresher Training	84
22.9 Training Records	85
22.10 Management Responsibilities	85
22.11 Reference Documents	85
22.12 Training and Staff Awareness Workflow	86

1. Company Information

Company Name: AG Group B.V.

Licence Number: OGL/2024/805/0287

Registered Address: Zuikertuintjeweg z/n, Curaçao

Purpose: Provision of online gaming services in accordance with applicable Curaçao regulations.

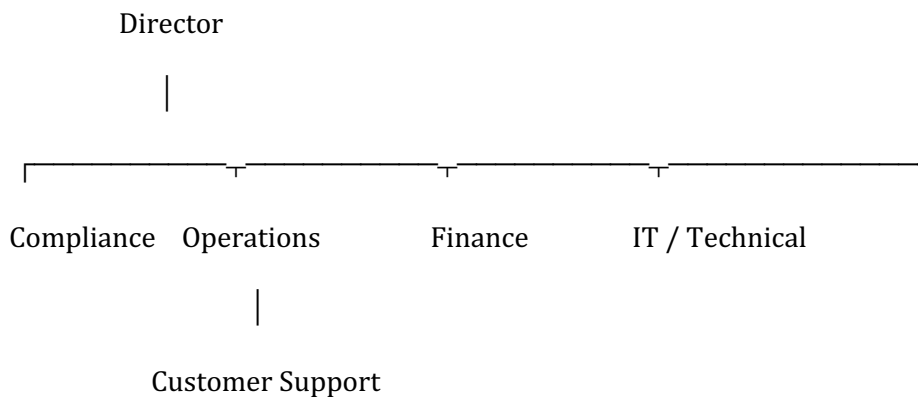
2. Organisational Structure

2.1 Overview

AG Group B.V. maintains an organisational structure designed to ensure effective operational management, regulatory compliance, financial oversight, customer protection, and information security. Responsibilities are clearly assigned to ensure proper segregation of duties and accountability across all business functions.

The Company periodically reviews its organisational structure to ensure it remains appropriate for the scale and nature of its business activities and complies with applicable regulatory requirements.

2.2 Organisation Structure



2.3 Roles and Responsibilities

Director

The Director has overall responsibility for the management of AG Group B.V., including:

- Overall business management
 - Corporate governance
 - Regulatory compliance oversight
 - Approval of internal policies and procedures
 - Risk management
 - Approval of significant operational decisions
-

Compliance

The Compliance function is responsible for ensuring that the Company complies with all applicable legal and regulatory requirements.

Responsibilities include:

- Monitoring regulatory developments
 - Maintaining compliance policies
 - AML/CFT oversight
 - KYC compliance monitoring
 - Regulatory reporting
 - Internal compliance reviews
 - Staff compliance awareness
-

Operations

The Operations function is responsible for the day-to-day operation of the Company's gaming platform.

Responsibilities include:

- Daily operational monitoring
 - Player account administration
 - Payment operations
 - Incident coordination
 - Operational reporting
 - Service quality monitoring
-

Finance

The Finance function is responsible for financial administration and payment management.

Responsibilities include:

- Financial record keeping
 - Payment reconciliation
 - Settlement monitoring
 - Expense management
 - Financial reporting
 - Supporting audit activities
-

Customer Support

Customer Support is responsible for assisting players and handling enquiries.

Responsibilities include:

- Player enquiries
 - Account assistance
 - Complaint handling
 - Responsible Gaming support
 - Escalation of unresolved issues
 - Maintaining communication records
-

IT / Technical

The IT function is responsible for maintaining the technical environment supporting the Company's operations.

Responsibilities include:

- System administration
 - Information security
 - Backup management
 - Access control
 - Incident response
 - System monitoring
 - Infrastructure maintenance
-

2.4 Segregation of Duties

To minimise operational and compliance risks, AG Group B.V. maintains an appropriate segregation of duties between operational, financial, compliance, customer support, and technical functions.

No single individual is responsible for initiating, approving, executing, and reviewing the same critical operational activity.

2.5 Reporting Lines

Each department reports to the Director through its designated department head. Material operational issues, compliance matters, financial risks, and security incidents shall be escalated promptly to senior management for review and decision-making.

3. Business Activities

3.1 Business Overview

AG Group B.V. is an online gaming operator licensed under the applicable laws and regulations of Curaçao. The Company is responsible for the operation and management of its online gaming business, ensuring that all activities are conducted in a secure, fair, transparent and compliant manner.

The Company is committed to maintaining high standards of operational integrity, customer protection, responsible gaming, anti-money laundering compliance, and information security.

3.2 Services Provided

AG Group B.V. provides online gaming services, including:

- Operation and management of online gaming services.
- Customer account registration and administration.
- Payment processing and settlement management.
- Responsible Gaming measures.
- Customer support services.

- Regulatory compliance and reporting.
- Protection of customer funds and personal data.

All services are operated in accordance with applicable laws, licence conditions and internal policies.

3.3 Operational Markets

AG Group B.V. provides its services only in jurisdictions where it is legally permitted to do so.

The Company monitors applicable legal and regulatory requirements and implements appropriate controls to restrict access from prohibited or restricted jurisdictions.

The Company reserves the right to suspend or terminate services in any jurisdiction where regulatory requirements cannot be satisfied.

3.4 Online Gaming Operations

The Company operates an online gaming platform that enables registered customers to:

- Register and maintain a player account.
- Access authorised online gaming services.
- Deposit and withdraw funds using approved payment methods.
- Review account balances and transaction history.
- Access responsible gaming tools.
- Contact customer support when assistance is required.

Operational procedures are continuously monitored to ensure service availability, integrity and compliance.

3.5 Player Account Management

The Company maintains secure player accounts for all registered customers.

Player account management includes:

- Customer registration.

- Identity verification (KYC).
- Account activation.
- Account suspension or closure where necessary.
- Balance management.
- Transaction history.
- Responsible Gaming controls.
- Account security monitoring.

Access to player accounts is restricted to authorised personnel only.

3.6 Payment Management

The Company maintains procedures for the secure processing of customer deposits, withdrawals and settlements.

Payment operations include:

- Verification of payment requests.
- Monitoring of payment transactions.
- Reconciliation of payment records.
- Protection of customer funds.
- Maintenance of payment records.
- Compliance with applicable financial and regulatory requirements.

Where payment collection or settlement services are performed by authorised third-party service providers, such activities are conducted under appropriate contractual arrangements and subject to ongoing oversight.

3.7 Responsible Gaming

AG Group B.V. is committed to promoting responsible gaming and protecting customers from gambling-related harm.

Responsible Gaming measures include:

- Minimum age verification.
- Self-exclusion options.
- Deposit limit functionality.
- Cooling-off periods.
- Reality check notifications.

- Customer support and guidance.

Further details are set out in the Company's Responsible Gaming Policy.

3.8 AML/CFT Compliance

AG Group B.V. maintains a comprehensive Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) framework.

The Company applies risk-based procedures including:

- Customer Due Diligence (CDD).
- Enhanced Due Diligence (EDD), where appropriate.
- Sanctions screening.
- Politically Exposed Person (PEP) screening.
- Transaction monitoring.
- Suspicious activity reporting.
- Record retention.

The AML/CFT framework is designed to comply with all applicable legal and regulatory obligations.

4. Governance and Responsibilities

4.1 Governance Framework

AG Group B.V. has established an internal governance framework to ensure that all business activities are conducted in accordance with applicable laws, licence conditions, internal policies and recognised industry standards.

The governance framework is designed to ensure:

- Clear allocation of responsibilities.
- Appropriate segregation of duties.
- Effective decision-making.
- Regulatory compliance.
- Risk management.
- Protection of customer interests.
- Operational integrity.

The Company periodically reviews its governance arrangements to ensure they remain appropriate for its business activities.

4.2 Roles and Responsibilities

Function	Primary Responsibilities
Director	Overall management, corporate governance, strategic decisions, approval of company policies and regulatory oversight.
Compliance	Regulatory compliance, AML/CFT oversight, policy implementation, regulatory reporting, compliance monitoring and internal reviews.
Operations	Daily operational management, service monitoring, operational reporting, incident coordination and business process management.
Finance	Financial administration, reconciliation, payment monitoring, accounting records and financial reporting.
Customer Support	Player enquiries, complaint handling, Responsible Gaming assistance and customer communication.

Information Technology	System administration, information security, infrastructure maintenance, backup management and technical support.
------------------------	---

4.3 Decision-Making Authority

Operational decisions are made in accordance with the Company's internal approval procedures.

Material decisions relating to regulatory compliance, financial matters, customer protection or operational risk shall be escalated to senior management for approval.

Where necessary, significant matters shall be documented and retained for audit purposes.

4.4 Segregation of Duties

AG Group B.V. maintains appropriate segregation of duties to minimise operational and compliance risks.

Critical activities are separated where reasonably practicable, including:

- Customer account administration.
- Payment processing.
- Financial reconciliation.
- Compliance monitoring.
- System administration.
- Approval of significant operational changes.

No individual should be solely responsible for initiating, approving and reviewing the same critical activity.

4.5 Internal Reporting

Operational departments shall report significant matters to management in a timely manner.

Examples include:

- Regulatory matters.
- Information security incidents.
- Customer complaints.
- AML/CFT alerts.
- Operational disruptions.
- Business continuity events.

Management shall review significant incidents and determine appropriate corrective actions.

4.6 Policy Review

The Company shall review its operational policies and procedures on a regular basis, and whenever there are:

- Changes in applicable legislation.
- Regulatory updates.
- Material operational changes.
- Information security incidents.
- Business process improvements.

Revised policies shall be approved by management before implementation.

5. Operational Procedures

5.1 Daily Operations

AG Group B.V. performs daily operational activities to ensure the continuous, secure and compliant operation of its online gaming services.

Daily operational activities include, but are not limited to:

- Monitoring the availability and performance of the gaming platform.
- Reviewing customer registrations and account activities.
- Processing deposits and withdrawal requests.
- Monitoring payment transactions and settlement activities.
- Responding to customer enquiries and support requests.
- Monitoring system alerts and operational incidents.

- Reviewing compliance alerts and suspicious activities.
 - Verifying successful completion of scheduled backups.
 - Monitoring third-party service availability.
 - Recording and escalating operational issues where necessary.
-

5.2 Customer Registration

All customers must complete the registration process before accessing the Company's gaming services.

The registration process includes:

- Submission of required personal information.
- Acceptance of the Terms and Conditions.
- Age verification.
- Risk assessment where applicable.
- Identity verification (KYC) when required.

Customer accounts shall only be activated after all applicable registration requirements have been satisfied.

5.3 Player Login and Account Access

Players may access their accounts using their registered credentials.

To protect customer accounts, the Company implements security measures including:

- Secure authentication.
 - Password protection.
 - Session management.
 - Monitoring of suspicious login activities.
 - Account restriction where suspicious activity is detected.
-

5.4 Deposit Procedures

Customers may deposit funds using approved payment methods.

Deposit procedures include:

- Verification of payment requests.
- Recording of payment transactions.
- Updating player account balances.
- Monitoring for suspicious transactions.
- Reconciliation with payment records.

Deposits may be delayed or rejected where additional verification is required.

5.5 Gaming Operations

Once logged in and funded, customers may participate in authorised gaming activities.

Operational controls include:

- Continuous system monitoring.
 - Transaction recording.
 - Session management.
 - Monitoring of abnormal activity.
 - Automatic logging of gaming transactions.
-

5.6 Withdrawal Procedures

Withdrawal requests are processed in accordance with the Company's internal procedures.

The withdrawal process includes:

- Verification of customer identity where required.
- Review of account status.
- AML/CFT review where applicable.
- Approval of withdrawal requests.
- Payment processing.
- Recording of completed transactions.

Withdrawals may be delayed where additional verification is necessary.

5.7 Customer Support

Customer Support is responsible for assisting customers regarding:

- Account enquiries.
- Payment enquiries.
- Responsible Gaming requests.
- Technical support.
- Complaint handling.
- General operational enquiries.

Customer communications are recorded where appropriate for quality assurance and regulatory purposes.

5.8 Account Suspension and Closure

The Company may suspend or close customer accounts where:

- Regulatory requirements require such action.
- KYC documentation cannot be completed.
- Fraud or suspicious activity is identified.
- AML/CFT concerns arise.
- Responsible Gaming measures require account restriction.
- The customer breaches the Terms and Conditions.

Appropriate records shall be maintained for all account suspension or closure decisions.

5.9 Operational Monitoring

Operational monitoring is performed on an ongoing basis to ensure system stability and regulatory compliance.

Monitoring activities include:

- Platform availability.
- Payment processing.
- Customer activity.
- Security alerts.
- System performance.
- Error logs.
- Backup status.
- Third-party service availability.

Material operational issues shall be investigated promptly.

5.10 Incident Escalation

Operational incidents shall be managed according to the Company's incident management procedures.

The escalation process includes:

1. Identification of the incident.
2. Initial assessment of severity.
3. Notification of relevant personnel.
4. Investigation and root cause analysis.
5. Corrective action.
6. Verification of resolution.
7. Documentation and management review.

Where required, significant incidents shall be reported to the relevant regulatory authority.

5.11 Daily Operational Checklist

The following activities are performed as part of the daily operational review:

- Review platform availability.
 - Review system alerts.
 - Verify successful backups.
 - Review payment processing status.
 - Monitor customer support tickets.
 - Review suspicious transaction alerts.
 - Confirm operational logs are retained.
 - Verify completion of scheduled maintenance.
 - Escalate any unresolved operational issues.
 - Record daily operational activities.
-

5.12 Operational Workflow

Player Registration



Identity Verification (KYC)



Account Activation



Player Login



Deposit



Gaming Activity



Withdrawal Request



Compliance Review (if required)



Payment Processing



Settlement



Transaction Record Retention

The operational workflow above summarises the standard customer journey and the principal operational procedures adopted by AG Group B.V. Additional verification, compliance reviews, or operational controls may be applied where required by law, regulation, or internal policies.

6. Customer Registration and KYC

6.1 Customer Registration

All customers must complete the registration process before accessing the Company's gaming services.

During registration, customers are required to provide accurate and complete information, including:

- Full name
- Date of birth
- Residential address
- Country of residence
- Nationality
- Email address
- Mobile telephone number (where applicable)

Customers must confirm that:

- They are at least 18 years of age, or the minimum legal age required in their jurisdiction.
- The information provided is accurate and complete.
- They agree to the Company's Terms and Conditions and Privacy Policy.

The Company reserves the right to refuse or suspend registration where inaccurate or misleading information is provided.

6.2 Identity Verification (KYC)

The Company applies Know Your Customer (KYC) procedures in accordance with applicable laws and regulatory requirements.

Identity verification may be conducted:

- Before processing withdrawals.
- Where required under AML/CFT regulations.
- When unusual account activity is identified.
- Where additional verification is considered necessary by the Company.

Customers may be required to provide one or more of the following documents:

- Government-issued photo identification (Passport, National ID Card or Driver's Licence).
- Proof of residential address issued within the previous three (3) months.
- Proof of ownership of the payment method, where applicable.
- Additional documentation reasonably requested by the Company.

Accounts may remain restricted until the verification process has been successfully completed.

6.3 Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) shall be applied where a customer presents a higher level of money laundering, terrorist financing or fraud risk.

Examples include:

- Politically Exposed Persons (PEPs).
- High-risk jurisdictions.
- Large or unusual transactions.
- Complex ownership structures.
- Customers identified as high-risk through internal risk assessments.

Additional information may be requested, including:

- Source of Funds.
- Source of Wealth.
- Occupation.
- Additional identity documentation.
- Additional proof of address.
- Supporting financial documentation.

The Company may decline to establish or continue a business relationship where satisfactory information cannot be obtained.

6.4 Ongoing Customer Monitoring

Customer information shall be reviewed periodically to ensure that it remains accurate and up to date.

The Company performs ongoing monitoring of:

- Customer transactions.
- Changes in customer risk profile.
- Suspicious activities.
- Payment behaviour.
- Account usage.

Where necessary, customers may be requested to provide updated KYC documentation.

6.5 Record Retention

All customer registration records and KYC documentation shall be maintained securely in accordance with the Company's Record Retention Policy and applicable legal requirements.

Access to customer information shall be restricted to authorised personnel only.

Customer records shall be retained for the period required by applicable law and regulatory requirements.

6.6 Registration and KYC Workflow

Registration

- KYC
- Risk Assessment
- Account Approval
- Ongoing Monitoring

The customer registration and KYC procedures described in this chapter shall be read together with the Company's AML/CFT Policy, Privacy Policy, Terms and Conditions, and applicable regulatory requirements.

7. AML/CFT Compliance

7.1 Overview

AG Group B.V. is committed to preventing money laundering, terrorist financing, fraud and other financial crimes.

The Company maintains a risk-based Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) programme in accordance with applicable laws, licence conditions and regulatory requirements.

The Company's AML/CFT framework is designed to:

- Prevent the misuse of the Company's services for financial crime.
 - Protect customers and the integrity of the gaming platform.
 - Detect and report suspicious activities.
 - Ensure compliance with applicable legal and regulatory obligations.
-

7.2 Risk-Based Approach

AG Group B.V. adopts a risk-based approach when assessing customer relationships and transactions.

Risk assessments consider factors including:

- Customer profile.
- Country of residence.
- Geographic risk.
- Transaction patterns.
- Payment methods.
- Source of funds.
- Gaming behaviour.
- Politically Exposed Person (PEP) status.
- Sanctions screening results.

Higher-risk customers are subject to additional monitoring and Enhanced Due Diligence procedures.

7.3 Customer Due Diligence (CDD)

Customer Due Diligence is performed in accordance with the Company's AML Policy.

CDD measures include:

- Customer identification.
- Identity verification.
- Age verification.

- Verification of residential address where required.
- Assessment of customer risk.
- Ongoing customer monitoring.

The Company reserves the right to request additional documentation at any time.

7.4 Enhanced Due Diligence (EDD)

Enhanced Due Diligence shall be applied where higher risks are identified.

EDD may include:

- Additional identity verification.
- Source of Funds verification.
- Source of Wealth verification.
- Additional proof of address.
- Enhanced transaction monitoring.
- Senior management approval where required.

The Company may refuse or terminate business relationships where satisfactory information cannot be obtained.

7.5 Transaction Monitoring

The Company continuously monitors customer transactions to identify unusual or suspicious activities.

Monitoring activities include:

- Unusually large deposits.
- High-frequency transactions.
- Structuring of transactions.
- Rapid deposits and withdrawals.
- Unusual betting patterns.
- Transactions involving high-risk jurisdictions.
- Any activity inconsistent with the customer's profile.

Alerts are reviewed by authorised personnel.

7.6 Sanctions and PEP Screening

Customers may be screened against:

- International sanctions lists.
- Politically Exposed Person (PEP) databases.
- Other applicable regulatory watchlists.

Positive matches shall be investigated before any business relationship is established or continued.

7.7 Suspicious Activity Reporting

Where suspicious activity is identified, the Company shall investigate the matter promptly.

Where required by law, Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs) shall be submitted to the relevant competent authority.

All investigations shall remain confidential.

7.8 Record Retention

The Company maintains AML/CFT records in accordance with applicable legal and regulatory requirements.

Records include:

- Customer identification documents.
- KYC documentation.
- Risk assessments.
- Transaction records.
- Monitoring records.
- Internal investigation records.
- Regulatory reports.

Records shall be retained for the minimum period required by applicable law.

7.9 Staff Training

Employees whose duties involve customer onboarding, payment processing, compliance or operational oversight shall receive AML/CFT training.

Training covers:

- Customer Due Diligence.
- Suspicious activity identification.
- Reporting obligations.
- Regulatory updates.
- Internal AML procedures.

Training records shall be maintained by the Company.

7.10 AML/CFT Workflow

Customer Registration

→ CDD

→ Risk Assessment

→ Transaction Monitoring

→ Suspicious Activity Review

→ Regulatory Reporting

→ Record Retention

7.11 Reference Documents

This chapter should be read together with:

- AML/CFT Policy
- Customer Due Diligence Procedures
- Record Retention Policy
- Terms and Conditions
- Privacy Policy

8. Responsible Gaming

8.1 Purpose

AG Group B.V. is committed to providing a safe, fair and responsible gaming environment.

The Company recognises that while online gaming is intended to be a form of entertainment, some customers may experience gambling-related harm. Accordingly, the Company has implemented a Responsible Gaming framework designed to promote informed gaming decisions and provide appropriate customer protection measures.

The Responsible Gaming programme forms an integral part of the Company's operational and regulatory compliance framework.

8.2 Responsible Gaming Principles

The Company is committed to the following principles:

- Preventing underage gaming.
 - Promoting responsible gaming behaviour.
 - Providing customers with tools to manage their gaming activity.
 - Protecting vulnerable customers.
 - Supporting customers who may experience gambling-related harm.
 - Complying with all applicable regulatory requirements.
-

8.3 Age Verification

Only customers who meet the minimum legal age requirement may register and use the Company's gaming services.

Age verification measures include:

- Customer declaration during registration.
- Identity verification where required.
- Account suspension if age verification cannot be completed.

Where underage gaming is identified, the Company shall immediately suspend or terminate the relevant account.

8.4 Responsible Gaming Tools

The Company provides customers with responsible gaming tools designed to assist them in managing their gaming activity.

These tools may include:

- Deposit limits.
- Self-exclusion.
- Cooling-off periods.
- Reality check notifications.
- Account closure upon request.

Customers may request these tools through their account settings or by contacting Customer Support.

8.5 Self-Exclusion

Customers may voluntarily exclude themselves from accessing the Company's gaming services.

Available self-exclusion periods include:

- 1 year
- 3 years
- 5 years
- 10 years
- Lifetime

During the self-exclusion period:

- Customer access shall be restricted.
- Marketing communications shall cease where applicable.
- The Company shall take reasonable steps to prevent account reactivation before the exclusion period expires.

Self-exclusion applies to all gaming activities operated by the Company.

8.6 Customer Support

Where customers indicate that they may be experiencing gambling-related harm, Customer Support personnel shall:

- Provide information regarding Responsible Gaming.
- Explain available Responsible Gaming tools.
- Assist with self-exclusion requests.
- Escalate matters where appropriate.

Customer Support personnel shall not provide financial advice or counselling services.

8.7 Staff Awareness

Employees involved in customer-facing activities receive periodic training regarding Responsible Gaming.

Training includes:

- Recognition of potential gambling-related harm.
 - Responsible Gaming procedures.
 - Customer communication.
 - Escalation procedures.
 - Internal reporting requirements.
-

8.8 Monitoring and Review

The Company periodically reviews the effectiveness of its Responsible Gaming programme.

Reviews may include:

- Customer feedback.
- Complaint trends.
- Self-exclusion statistics.
- Regulatory developments.
- Internal compliance reviews.

Where improvements are identified, appropriate updates shall be implemented.

8.9 Reference Documents

The Responsible Gaming procedures described in this Manual shall be read together with the Company's:

- Responsible Gaming Policy
 - Terms and Conditions
 - Privacy Policy
 - Player Complaints Policy
-

8.10 Responsible Gaming Workflow

Customer Registration



Age Verification



Gaming Activities



Responsible Gaming Monitoring



Responsible Gaming Tools



Customer Support



Account Restriction

9. Player Complaints Handling

9.1 Purpose

AG Group B.V. is committed to providing a fair, transparent and efficient process for handling customer complaints.

The Company encourages customers to raise concerns promptly so that issues can be investigated and resolved in a timely manner. All complaints are handled objectively, confidentially and in accordance with applicable regulatory requirements.

9.2 Scope

This procedure applies to all complaints relating to the Company's online gaming services, including but not limited to:

- Account-related issues.
 - Deposit and withdrawal enquiries.
 - Payment disputes.
 - Bonus and promotional disputes.
 - Responsible Gaming requests.
 - Technical issues affecting gameplay.
 - Customer service complaints.
 - Privacy or personal data concerns.
 - Any other operational matters relating to the Company's services.
-

9.3 Complaint Submission

Customers may submit complaints through the Company's official customer support channels, including:

- Email.
- Live Chat (if available).
- Online Contact Form (if available).

Customers should provide sufficient information to enable the Company to investigate the matter, including:

- Player username.
 - Date and time of the incident.
 - Description of the issue.
 - Supporting evidence, where available.
-

9.4 Complaint Investigation

Upon receipt of a complaint, the Company shall:

- Acknowledge receipt of the complaint.
- Review the relevant account and transaction records.
- Obtain additional information where necessary.
- Investigate the matter objectively.
- Determine the appropriate resolution.

Where required, relevant departments may be consulted during the investigation.

9.5 Complaint Resolution

The Company aims to resolve complaints as promptly as reasonably practicable.

Possible outcomes include:

- Explanation of the Company's decision.
- Correction of administrative errors.
- Adjustment of account records where appropriate.
- Reimbursement where applicable.
- Rejection of unsupported claims.

Customers shall be informed of the outcome together with the reasons for the decision.

9.6 Escalation

Where a complaint cannot be resolved through the normal investigation process, the matter shall be escalated to senior management or the Compliance function for further review.

Where applicable, customers may be informed of any available external dispute resolution mechanisms in accordance with applicable regulatory requirements.

9.7 Record Retention

The Company maintains records of all complaints, including:

- Complaint details.
- Investigation notes.

- Supporting evidence.
- Decisions made.
- Customer communications.
- Resolution date.

Complaint records shall be retained in accordance with the Company's Record Retention Policy.

9.8 Monitoring and Continuous Improvement

Complaint trends are periodically reviewed to identify recurring issues and opportunities for improvement.

The Company may implement corrective actions, update internal procedures or provide additional staff training where necessary to enhance service quality and customer satisfaction.

9.9 Reference Documents

This chapter should be read together with the following documents:

- Player Complaints Policy
 - Responsible Gaming Policy
 - Terms and Conditions
 - Privacy Policy
-

9.10 Complaint Handling Workflow

Customer Complaint

→ Complaint Received

→ Investigation

→ Internal Review

→ Resolution

→ Customer Notification

→ Record Retention

10. Payment Processing and Fund Management

10.1 Purpose

AG Group B.V. has established payment processing and fund management procedures to ensure that all customer funds are handled securely, accurately and in compliance with applicable legal and regulatory requirements.

The Company implements appropriate controls to safeguard customer funds, maintain accurate financial records and support transparent payment operations.

10.2 Accepted Payment Methods

The Company accepts payment methods that have been approved through its internal due diligence procedures.

Payment methods may include:

- Bank Transfer
- Credit / Debit Cards
- Electronic Wallets
- Other approved payment solutions

The Company periodically reviews payment providers to ensure continued compliance with regulatory and operational requirements.

10.3 Deposit Procedures

Customer deposits are processed through authorised payment channels.

The deposit process includes:

- Verification of the payment request.
- Confirmation of successful payment.
- Recording of the transaction.
- Updating the customer's account balance.
- Monitoring for unusual or suspicious activity.

Where necessary, additional verification may be requested before funds are credited to a customer account.

10.4 Withdrawal Procedures

Withdrawal requests are subject to internal verification procedures before payment is processed.

The Company may perform the following checks:

- Customer identity verification.
- Completion of KYC requirements.
- AML/CFT review.
- Verification of payment method ownership.
- Review of account status and transaction history.

Approved withdrawals are processed using the customer's verified payment method.

10.5 Payment Monitoring

The Company continuously monitors payment activities to identify unusual transactions or operational issues.

Monitoring activities include:

- Large or unusual deposits.
- High-frequency payment activity.
- Failed payment transactions.
- Chargeback activity.
- Payment fraud indicators.
- Unusual withdrawal behaviour.

Where appropriate, payment activities may be escalated for further review.

10.6 Customer Funds

The Company maintains procedures designed to protect customer funds and ensure accurate financial reconciliation.

Customer funds are:

- Properly recorded.
- Subject to reconciliation procedures.
- Protected against unauthorised access.
- Processed only through authorised payment channels.

Access to payment records is restricted to authorised personnel.

Where payment processing services are provided by authorised third-party service providers, AG Group B.V. maintains appropriate oversight and contractual arrangements to ensure that such services are performed in accordance with applicable legal, regulatory and operational requirements.

10.7 Reconciliation

Financial reconciliation is performed on a regular basis to ensure the accuracy and completeness of payment records.

Reconciliation activities include:

- Deposit reconciliation.
- Withdrawal reconciliation.
- Payment provider reconciliation.
- Internal financial reconciliation.
- Investigation of discrepancies.

Any discrepancies identified during reconciliation shall be investigated and resolved promptly.

10.8 Payment Security

The Company applies security controls to protect payment information and financial transactions.

Security measures include:

- Restricted system access.
- Secure transmission of payment information.
- Transaction logging.

- Access monitoring.
- Periodic security reviews.

Sensitive financial information is protected in accordance with the Company's Information Security and Privacy policies.

10.9 Record Retention

Payment records are maintained in accordance with applicable legal and regulatory requirements.

Records include:

- Deposit records.
- Withdrawal records.
- Settlement records.
- Reconciliation reports.
- Payment investigations.
- Financial audit records.

Records shall be retained for the minimum period required by applicable law.

10.10 Reference Documents

This chapter should be read together with:

- AML/CFT Policy
 - Terms and Conditions
 - Privacy Policy
 - Information Security Policy (if applicable)
-

10.11 Payment Processing Workflow

Customer Deposit

→ Payment Verification

→ Account Balance Updated

- Gaming Activities
- Withdrawal Request
- KYC / AML Review (if required)
- Payment Approval
- Payment Processing
- Transaction Recording
- Reconciliation

11. Personal Data Protection

11.1 Purpose

AG Group B.V. is committed to protecting the privacy and personal data of its customers. The Company processes personal data in accordance with applicable data protection laws, regulatory requirements and internal policies.

Appropriate administrative, technical and organisational measures have been implemented to ensure that personal data is processed securely, lawfully and only for legitimate business purposes.

11.2 Collection of Personal Data

The Company collects personal data only where necessary for the operation of its gaming services and compliance with applicable legal and regulatory obligations.

Personal data collected may include:

- Full name
- Date of birth
- Residential address
- Email address
- Telephone number
- Identification documents
- Payment information
- Gaming activity records
- Customer support communications

The Company collects only the information necessary for the intended purpose.

11.3 Use of Personal Data

Personal data may be processed for the following purposes:

- Customer registration and account management.
- Identity verification (KYC).
- AML/CFT compliance.
- Processing deposits and withdrawals.
- Customer support.
- Fraud prevention.
- Regulatory reporting.
- Responsible Gaming measures.
- Compliance with legal obligations.

Personal data shall not be used for purposes incompatible with the reasons for which it was collected.

11.4 Data Security

The Company implements appropriate security measures to protect personal data against unauthorised access, disclosure, alteration or destruction.

Security measures include:

- Access control based on job responsibilities.
- Password protection.
- Encryption of sensitive information where appropriate.
- Secure data transmission.
- Audit logging.
- Periodic security reviews.

Only authorised personnel may access customer information.

11.5 Data Retention

Personal data shall be retained only for as long as necessary to satisfy legal, regulatory and operational requirements.

Retention periods take into account:

- Applicable laws.
- Regulatory obligations.
- AML/CFT requirements.
- Audit requirements.
- Dispute resolution.

When the retention period expires, personal data shall be securely deleted or anonymised where appropriate.

11.6 Data Sharing

Personal data may be shared only where necessary and permitted by applicable law.

Examples include:

- Regulatory authorities.
- Law enforcement agencies.
- Payment service providers.
- Identity verification service providers.
- Professional advisers.
- Technology service providers acting on behalf of the Company.

Appropriate safeguards shall be implemented when personal data is shared with third parties.

11.7 Data Subject Rights

Customers may exercise their rights in accordance with applicable data protection laws.

Where applicable, customers may request:

- Access to their personal data.
- Correction of inaccurate information.
- Deletion of personal data where legally permissible.
- Restriction of processing.

- Withdrawal of consent where applicable.

Requests shall be handled in accordance with the Company's Privacy Policy and applicable legal requirements.

11.8 Confidentiality

Employees, contractors and authorised third-party service providers who have access to personal data are required to maintain confidentiality and comply with the Company's data protection requirements.

Unauthorised disclosure of personal information is strictly prohibited.

11.9 Reference Documents

This chapter should be read together with:

- Privacy Policy
 - AML/CFT Policy
 - Terms and Conditions
 - Information Security Policy (if applicable)
-

11.10 Personal Data Protection Workflow

Customer Registration

→ Personal Data Collection

→ Secure Storage

→ Operational Use

→ Regulatory Compliance

→ Data Retention

→ Secure Deletion / Anonymisation

12. Information Security

12.1 Purpose

AG Group B.V. is committed to maintaining a secure operational environment to protect its information assets, customer data, systems and services from unauthorised access, misuse, alteration, disclosure or destruction.

The Company implements appropriate administrative, technical and organisational security measures to ensure the confidentiality, integrity and availability of information.

12.2 Information Security Objectives

The Company's information security programme aims to:

- Protect customer information.
- Maintain system availability.
- Prevent unauthorised access.
- Ensure data integrity.
- Reduce operational and cybersecurity risks.
- Support regulatory compliance.

Information security controls are reviewed periodically to ensure their continued effectiveness.

12.3 Access Control

Access to systems and information is granted only to authorised personnel based on their job responsibilities.

The Company applies the following controls:

- Role-based access permissions.
- Individual user accounts.
- Strong password requirements.
- Periodic access reviews.
- Prompt removal of access for departed personnel.

Administrative access is restricted to authorised personnel only.

12.4 Authentication and Password Security

The Company requires users with system access to maintain secure authentication credentials.

Security measures include:

- Unique user accounts.
- Strong password policies.
- Periodic password updates where applicable.
- Protection against unauthorised password disclosure.
- Account lockout following repeated unsuccessful login attempts, where technically supported.

Passwords must never be shared with unauthorised persons.

12.5 Network and System Security

The Company implements technical measures to protect its systems and network infrastructure.

These measures include:

- Firewalls.
- Secure network configuration.
- System monitoring.
- Malware protection.
- Regular software updates.
- Patch management.

Only authorised systems may connect to the Company's operational environment.

12.6 Data Security

The Company protects customer and operational data through appropriate security controls.

Data protection measures include:

- Secure storage.
- Encryption of sensitive information where appropriate.
- Controlled access.
- Backup procedures.
- Secure disposal of information.

Data integrity is maintained through regular monitoring and verification procedures.

12.7 Logging and Monitoring

The Company maintains system logs to support operational monitoring, troubleshooting and regulatory compliance.

Logs may include:

- User authentication.
- Administrative activities.
- Payment activities.
- System events.
- Security events.
- Operational incidents.

Log access is restricted to authorised personnel.

12.8 Security Incident Management

Security incidents shall be reported and managed in accordance with the Company's incident management procedures.

The Company shall:

- Identify the incident.
- Assess the impact.
- Contain the incident.
- Investigate the root cause.
- Implement corrective actions.
- Review preventive measures.

Where required by applicable law, material incidents shall be reported to the relevant regulatory authority.

12.9 Backup and Recovery

The Company performs regular backups of critical operational information to support business continuity and disaster recovery.

Backup procedures include:

- Scheduled backups.
- Secure storage of backup data.
- Periodic verification of backup integrity.
- Recovery testing where appropriate.

Backup access is restricted to authorised personnel.

12.10 Security Awareness

Employees are expected to comply with the Company's information security requirements.

Where appropriate, employees receive training regarding:

- Password security.
 - Phishing awareness.
 - Data protection.
 - Incident reporting.
 - Confidentiality obligations.
-

12.11 Reference Documents

This chapter should be read together with:

- Privacy Policy
- AML/CFT Policy
- Business Continuity Plan
- Disaster Recovery Procedures
- Record Retention Policy (if applicable)

12.12 Information Security Workflow

System Access Request

- User Authentication
- Access Authorisation
- Operational Activities
- System Monitoring
- Security Event Detection
- Incident Response (if required)
- Audit Logging
- Periodic Security Review

13. Business Continuity

13.1 Purpose

AG Group B.V. has established a Business Continuity Management (BCM) framework to ensure that critical business operations can continue with minimal disruption in the event of unexpected incidents.

The objective of the BCM programme is to minimise operational interruptions, protect customers, safeguard company assets, and ensure compliance with applicable legal and regulatory requirements.

13.2 Scope

The Business Continuity Management framework applies to all critical business operations, including:

- Online gaming operations
- Customer account management
- Payment processing
- Customer support
- Regulatory compliance
- Information technology services
- Information security

- Financial operations
-

13.3 Business Continuity Objectives

The Company aims to:

- Maintain the availability of critical services.
 - Minimise disruption to customers.
 - Protect customer funds and personal information.
 - Ensure regulatory compliance during operational disruptions.
 - Restore normal operations as quickly as reasonably practicable.
 - Reduce operational and financial risks.
-

13.4 Business Continuity Planning

Business continuity plans are established to address situations including:

- Power outages
- Internet or telecommunications failures
- Hardware failures
- Software failures
- Cybersecurity incidents
- Third-party service interruptions
- Natural disasters
- Pandemic or public health emergencies
- Loss of key personnel

Each plan identifies:

- Critical business functions.
 - Responsible personnel.
 - Communication procedures.
 - Temporary operating arrangements.
 - Recovery priorities.
-

13.5 Roles and Responsibilities

Business continuity responsibilities are allocated as follows:

Function	Responsibilities
Director	Overall oversight and approval of business continuity plans.
Operations	Coordinate operational recovery and service continuity.
Compliance	Assess regulatory impact and coordinate regulatory notifications where required.
IT	Restore systems, infrastructure and technical services.
Customer Support	Communicate with customers regarding service interruptions.
Finance	Monitor payment operations and financial continuity.

13.6 Communication During Disruptions

In the event of a significant operational disruption, the Company shall:

- Notify relevant internal personnel.
- Assess the operational impact.
- Implement business continuity procedures.
- Provide updates to affected customers where appropriate.

- Notify regulators where required by applicable laws or licence conditions.
 - Maintain records of all communications.
-

13.7 Periodic Review and Testing

Business continuity plans shall be reviewed periodically and updated whenever:

- Business operations change.
- New risks are identified.
- Regulatory requirements are updated.
- Significant incidents occur.

Where appropriate, business continuity procedures shall be tested to verify their effectiveness.

13.8 Documentation and Record Keeping

The Company maintains documentation relating to:

- Business continuity plans.
- Testing results.
- Incident reports.
- Corrective actions.
- Management reviews.

These records are retained in accordance with the Company's Record Retention Policy.

13.9 Reference Documents

This chapter should be read together with:

- Disaster Recovery Procedures
 - Information Security Policy
 - Incident Management Procedures
 - Record Retention Policy
 - AML/CFT Policy
-

13.10 Business Continuity Workflow

Operational Disruption

- Initial Assessment
- Activate Business Continuity Plan
- Maintain Critical Operations
- Internal & External Communication
- Restore Normal Operations
- Management Review
- Continuous Improvement

13.11 Technical Infrastructure Overview

AG Group B.V. maintains a secure technical infrastructure to support the continuous operation of its gaming platform and related services.

The infrastructure is designed to ensure system availability, data integrity, operational resilience and regulatory compliance.

The technical environment consists of the following key components:

- Gaming Website / Web Portal
- Application Server
- Database Server
- Secure Backup Storage
- Monitoring and Logging Systems
- Third-party Payment Service Providers
- Disaster Recovery Environment

The Company performs continuous monitoring and routine maintenance to ensure that critical systems remain operational and that recovery procedures can be activated when necessary.

Players



Gaming Website

↓

Application Server

↓

Database Server

↓

Encrypted Backup Storage

Payment Service Providers

↕

Application Server

Monitoring & Logging

↓

Compliance / IT Team

Disaster Recovery Environment

↓

Business Continuity

14. Disaster Recovery

14.1 Purpose

AG Group B.V. has established Disaster Recovery (DR) procedures to ensure the timely recovery of critical information systems, operational data, and supporting infrastructure following a disruptive event.

The objective of the Disaster Recovery Plan is to minimise service interruption, protect customer information, maintain operational integrity, and support business continuity.

14.2 Scope

The Disaster Recovery procedures apply to all critical systems supporting the Company's operations, including:

- Gaming platform
 - Customer account systems
 - Payment processing systems
 - Databases
 - Network infrastructure
 - Backup systems
 - Internal operational systems
-

14.3 Disaster Recovery Objectives

The Company aims to:

- Restore critical systems as quickly as reasonably practicable.
 - Protect customer information and operational data.
 - Minimise operational downtime.
 - Prevent unnecessary data loss.
 - Maintain compliance with applicable regulatory requirements.
 - Ensure service continuity following a disruptive event.
-

14.4 Disaster Recovery Events

The Disaster Recovery Plan may be activated in response to events including:

- Hardware failure
- Server failure
- Database corruption
- Network outages
- Cybersecurity incidents
- Ransomware attacks
- Power failures
- Fire or natural disasters
- Failure of critical third-party infrastructure

The Company shall assess the severity of each incident before activating the Disaster Recovery Plan.

14.5 Backup Procedures

The Company performs regular backups of critical operational information.

Backup procedures include:

- Scheduled backups of critical systems and databases.
- Secure storage of backup data.
- Protection against unauthorised access.
- Verification of backup integrity.
- Periodic review of backup procedures.

Backup media shall be protected against loss, damage or unauthorised disclosure.

14.6 Recovery Procedures

Following activation of the Disaster Recovery Plan, the Company shall:

1. Assess the incident.
2. Identify affected systems.
3. Activate recovery procedures.
4. Restore critical systems.
5. Verify data integrity.
6. Resume operational services.
7. Monitor system stability.
8. Conduct post-recovery review.

Priority shall be given to systems supporting customer accounts, payment processing, and regulatory compliance.

14.7 Recovery Testing

The Company periodically reviews and tests its Disaster Recovery procedures to ensure their effectiveness.

Testing may include:

- Backup restoration.
- System recovery.
- Data integrity verification.
- Operational readiness assessment.

Results of testing shall be documented and reviewed by management.

14.8 Roles and Responsibilities

Function	Responsibility
Director	Overall oversight and approval of Disaster Recovery activities.
IT	Restore systems, infrastructure, databases and backups.
Operations	Coordinate operational recovery and business resumption.
Compliance	Assess regulatory obligations and coordinate required notifications.
Customer Support	Communicate with customers regarding service disruptions where appropriate.

14.9 Documentation and Record Keeping

The Company shall maintain records relating to:

- Disaster Recovery activations.
- Recovery activities performed.
- Recovery testing.
- Incident reports.
- Corrective actions.
- Lessons learned.

These records shall be retained in accordance with the Company's Record Retention Policy.

14.10 Reference Documents

This chapter should be read together with:

- Business Continuity Management
 - Information Security
 - Incident Management
 - Record Retention Policy
-

14.11 Disaster Recovery Workflow

Disruptive Event

- Incident Assessment
- Disaster Recovery Plan Activated
- System Recovery
- Data Verification
- Service Restoration
- System Monitoring
- Post-Incident Review

14.12 Continuous Improvement

Following each Disaster Recovery event or recovery test, the Company shall review the effectiveness of its Disaster Recovery procedures and implement improvements where necessary. The Disaster Recovery Plan shall be reviewed at least annually or whenever significant operational or technological changes occur.

15. Record Retention

15.1 Purpose

AG Group B.V. maintains records in accordance with applicable legal, regulatory, operational and business requirements.

The purpose of the Company's record retention programme is to ensure that business records remain complete, accurate, secure and readily available for regulatory review, audits, investigations and operational purposes.

15.2 Scope

This policy applies to all operational records created or maintained by the Company, including electronic records and supporting documentation.

The Company maintains records relating to:

- Customer registration.
 - KYC documentation.
 - AML/CFT records.
 - Payment transactions.
 - Financial records.
 - Customer complaints.
 - Responsible Gaming requests.
 - Operational reports.
 - Information security events.
 - Audit records.
 - Regulatory correspondence.
-

15.3 Record Retention Period

Records shall be retained for the minimum period required by applicable law and regulatory requirements.

Unless a longer period is required by law or regulatory authorities, the Company generally applies the following retention periods:

Record Type	Minimum Retention Period
Customer Registration Records	5 years
KYC Documentation	5 years
AML/CFT Records	5 years
Payment & Financial Records	5 years
Gaming Transaction Records	5 years
Customer Complaints	5 years
Responsible Gaming Records	5 years
Operational Logs	5 years
Security Incident Records	5 years

Regulatory Correspondence	5 years
---------------------------	---------

Where litigation, regulatory investigations or disputes are ongoing, records shall be retained until the matter has been fully resolved.

15.4 Record Protection

The Company implements appropriate measures to protect records against:

- Unauthorised access.
- Loss or theft.
- Accidental deletion.
- Damage or corruption.
- Unauthorised modification.

Electronic records are stored securely and access is limited to authorised personnel based on business responsibilities.

15.5 Access to Records

Access to company records is restricted to authorised personnel.

Access permissions are granted according to operational responsibilities and are reviewed periodically.

Regulatory authorities may be granted access to relevant records where required by applicable law.

15.6 Record Disposal

When the applicable retention period expires, records shall be securely disposed of in a manner that prevents unauthorised access or recovery.

The disposal process may include:

- Secure deletion of electronic records.
- Permanent destruction of physical records.
- Verification that disposal has been completed.

Where records remain subject to legal or regulatory requirements, disposal shall be postponed until such requirements have been satisfied.

15.7 Monitoring and Review

The Company periodically reviews its record retention practices to ensure continued compliance with legal, regulatory and operational requirements.

Where necessary, retention periods may be revised to reflect changes in applicable legislation or regulatory guidance.

15.8 Reference Documents

This chapter should be read together with:

- AML/CFT Policy
 - Privacy Policy
 - Information Security Procedures
 - Player Complaints Policy
 - Responsible Gaming Policy
-

15.9 Record Retention Workflow

Business Activity

→ Record Creation

→ Secure Storage

→ Authorised Access

→ Periodic Review

→ Retention Period

→ Secure Disposal

16. Regulatory Reporting

16.1 Purpose

AG Group B.V. is committed to maintaining open, transparent and timely communication with the Curaçao Gaming Authority (CGA) and other competent regulatory authorities.

The Company shall comply with all applicable regulatory reporting obligations arising from its gaming licence, applicable laws and regulatory requirements.

16.2 Regulatory Reporting Responsibilities

The Company shall ensure that all required regulatory reports are prepared accurately and submitted within the applicable deadlines.

Regulatory reporting responsibilities include:

- Submission of information requested by the Curaçao Gaming Authority.
- Notification of material operational or regulatory matters.
- Cooperation with regulatory inspections and audits.
- Provision of supporting documents where requested.
- Maintenance of complete regulatory records.

The Compliance function is responsible for coordinating regulatory communications and ensuring that reporting obligations are fulfilled.

16.3 Regulatory Notifications

Where required by applicable laws or licence conditions, the Company shall notify the relevant regulatory authority of material events, including but not limited to:

- Significant operational disruptions.
- Material security incidents.
- Changes affecting regulatory compliance.
- Significant changes to corporate information.
- Other reportable events as required by applicable regulations.

Notifications shall be submitted within the applicable regulatory timeframes.

16.4 Regulatory Inspections and Audits

The Company shall cooperate fully with regulatory inspections, reviews and audits.

Upon request, the Company shall make available:

- Operational records.
 - Customer records, where legally permitted.
 - Financial records.
 - Compliance documentation.
 - Internal policies and procedures.
 - Other information required by the competent authority.
-

16.5 Record Keeping

Copies of all regulatory submissions and correspondence shall be maintained securely.

Records include:

- Regulatory reports.
- Correspondence with regulatory authorities.
- Audit findings.
- Corrective action plans.
- Regulatory approvals.
- Supporting documentation.

Records shall be retained in accordance with the Company's Record Retention Policy.

16.6 Internal Review

Before submission, regulatory reports shall be reviewed by the appropriate personnel to ensure:

- Accuracy.
- Completeness.
- Consistency.
- Compliance with applicable regulatory requirements.

Where necessary, senior management approval shall be obtained prior to submission.

16.7 Continuous Compliance

The Company monitors changes in applicable laws, regulations and licence conditions.

Where regulatory requirements change, the Company shall:

- Review existing policies and procedures.
 - Update operational processes where necessary.
 - Provide additional staff guidance or training.
 - Maintain documentation demonstrating compliance.
-

16.8 Reference Documents

This chapter should be read together with:

- AML/CFT Policy
 - Responsible Gaming Policy
 - Privacy Policy
 - Record Retention Procedures
 - Internal Compliance Procedures
-

16.9 Regulatory Reporting Workflow

Regulatory Requirement

→ Internal Review

→ Document Preparation

→ Management Approval

→ Submission to Regulatory Authority

→ Regulatory Correspondence

→ Record Retention

→ Ongoing Compliance Monitoring

17. Internal Controls

17.1 Purpose

AG Group B.V. has established an internal control framework to ensure that its operations are conducted efficiently, securely and in compliance with applicable legal and regulatory requirements.

The internal control framework supports sound corporate governance, protects customer interests, safeguards Company assets and promotes operational integrity.

17.2 Internal Control Objectives

The Company's internal control framework aims to:

- Ensure compliance with applicable laws and regulations.
 - Protect customer funds and personal data.
 - Maintain accurate financial and operational records.
 - Prevent fraud and unauthorised activities.
 - Promote accountability and transparency.
 - Identify and manage operational risks.
 - Support continuous improvement of business operations.
-

17.3 Segregation of Duties

The Company applies segregation of duties to minimise operational and compliance risks.

Where reasonably practicable, critical responsibilities are separated to ensure that no individual has complete control over an entire operational process.

Examples include:

- Customer account administration.
- Payment approval and reconciliation.
- Financial record keeping.
- Compliance monitoring.
- System administration.

- Regulatory reporting.

Where complete segregation is not possible due to organisational size, compensating controls and management oversight shall be implemented.

17.4 Approval Controls

Certain operational activities require management approval before implementation.

Examples include:

- Material operational changes.
- Policy updates.
- Significant customer account actions.
- High-value financial transactions.
- Third-party service provider engagement.
- Regulatory submissions.

Approvals shall be documented where appropriate.

17.5 Operational Monitoring

The Company continuously monitors operational activities to identify irregularities and ensure compliance with internal procedures.

Monitoring activities include:

- Customer account activities.
- Payment transactions.
- Operational incidents.
- Customer complaints.
- Information security events.
- Compliance alerts.

Material issues shall be investigated promptly and escalated where necessary.

17.6 Risk Assessment

The Company periodically assesses operational risks that may affect its business activities.

Risk assessments consider:

- Operational risks.
- Financial risks.
- Information security risks.
- Compliance risks.
- Third-party risks.
- Reputational risks.

Where risks are identified, appropriate mitigation measures shall be implemented.

17.7 Internal Reviews

Management performs periodic internal reviews to evaluate the effectiveness of operational procedures and internal controls.

Reviews may include:

- Compliance with Company policies.
- Regulatory compliance.
- Operational performance.
- Information security controls.
- Payment processes.
- Customer complaint trends.
- Responsible Gaming measures.

Recommendations arising from internal reviews shall be documented and implemented where appropriate.

17.8 Corrective Actions

Where deficiencies or control weaknesses are identified, the Company shall implement appropriate corrective actions.

Corrective actions may include:

- Updating internal procedures.
- Strengthening operational controls.

- Additional employee training.
- System improvements.
- Enhanced monitoring activities.

Management shall review the effectiveness of corrective actions after implementation.

17.9 Documentation and Record Keeping

The Company maintains records relating to internal control activities, including:

- Risk assessments.
- Internal review reports.
- Corrective action plans.
- Approval records.
- Operational monitoring reports.

These records are retained in accordance with the Company's Record Retention Policy.

17.10 Reference Documents

This chapter should be read together with:

- AML/CFT Policy
 - Responsible Gaming Policy
 - Privacy Policy
 - Record Retention Policy
 - Information Security Procedures
-

17.11 Internal Control Workflow

Business Operations

→ Operational Monitoring

→ Risk Assessment

→ Internal Review

→ Corrective Actions

→ Management Approval

→ Record Retention

→ Continuous Improvement

18. Incident Management

18.1 Purpose

AG Group B.V. has established an Incident Management framework to ensure that operational incidents are identified, assessed, managed, documented and resolved in a timely and effective manner.

The objectives of the Incident Management process are to:

- Minimise disruption to business operations.
 - Protect customers and company assets.
 - Maintain regulatory compliance.
 - Restore normal operations as quickly as reasonably practicable.
 - Prevent similar incidents from recurring.
-

18.2 Scope

This procedure applies to all operational incidents affecting the Company's business activities, including but not limited to:

- System failures.
 - Network disruptions.
 - Payment processing issues.
 - Customer account issues.
 - Information security incidents.
 - Data protection incidents.
 - Service interruptions.
 - Third-party service failures.
 - Operational errors.
 - Regulatory compliance issues.
-

18.3 Incident Identification

Operational incidents may be identified through:

- System monitoring.
- Customer reports.
- Internal staff reports.
- Compliance monitoring.
- Security alerts.
- Third-party service providers.
- Routine operational reviews.

All employees are responsible for reporting incidents promptly.

18.4 Incident Classification

Incidents shall be assessed based on their:

- Operational impact.
- Financial impact.
- Customer impact.
- Regulatory impact.
- Information security impact.
- Business continuity impact.

Incidents may be classified as:

- Low
- Medium
- High
- Critical

The classification determines the required response and escalation procedures.

18.5 Incident Response

Upon identification of an incident, the Company shall:

1. Record the incident.
2. Assess the severity.
3. Notify the appropriate personnel.
4. Contain the incident where possible.

5. Investigate the root cause.
 6. Implement corrective actions.
 7. Restore normal operations.
 8. Monitor the effectiveness of the corrective actions.
-

18.6 Escalation Procedures

Significant incidents shall be escalated to management without unnecessary delay.

Examples include:

- Extended service outages.
- Material payment failures.
- Information security incidents.
- Significant customer impact.
- Regulatory compliance issues.
- Suspected fraud.

Where required, the Company shall notify the relevant regulatory authority in accordance with applicable legal and regulatory requirements.

18.7 Incident Documentation

The Company maintains records of all significant incidents.

Incident records include:

- Date and time.
 - Description.
 - Classification.
 - Root cause.
 - Corrective actions.
 - Resolution date.
 - Management review.
 - Regulatory reporting (where applicable).
-

18.8 Post-Incident Review

Following resolution of a significant incident, the Company shall conduct a post-incident review to evaluate:

- Root cause.
- Effectiveness of the response.
- Operational impact.
- Customer impact.
- Opportunities for improvement.

Recommendations shall be documented and implemented where appropriate.

18.9 Continuous Improvement

Incident trends shall be reviewed periodically to identify recurring issues.

The Company shall use incident analysis to improve:

- Operational procedures.
 - Information security.
 - Business continuity.
 - Disaster recovery.
 - Staff awareness.
 - Internal controls.
-

18.10 Reference Documents

This chapter should be read together with:

- Information Security
 - Business Continuity Management
 - Disaster Recovery Procedures
 - Internal Controls
 - Record Retention Policy
-

18.11 Incident Management Workflow

Incident Identified

- Incident Reported
- Initial Assessment
- Incident Classification
- Investigation
- Corrective Action
- Service Restoration
- Post-Incident Review
- Record Retention
- Continuous Improvement

19. Third-Party Service Providers

19.1 Purpose

AG Group B.V. engages third-party service providers where appropriate to support its business operations. The Company maintains appropriate oversight to ensure that outsourced services are performed in a secure, reliable and compliant manner.

The objective of this chapter is to establish procedures for the selection, management and ongoing monitoring of third-party service providers.

19.2 Scope

This chapter applies to all third-party service providers engaged by the Company to support its business activities, including but not limited to:

- Payment service providers.
- Cloud and hosting providers.
- Information technology service providers.
- Customer verification service providers.
- Professional advisers.
- Other outsourced operational service providers.

The Company remains responsible for ensuring that outsourced activities comply with applicable legal and regulatory requirements.

19.3 Selection and Due Diligence

Before engaging a third-party service provider, the Company shall conduct appropriate due diligence to assess the provider's suitability.

The assessment may include:

- Business reputation.
- Relevant licences or regulatory status, where applicable.
- Financial stability.
- Technical capability.
- Information security controls.
- Data protection measures.
- Operational reliability.
- Compliance with applicable laws.

The Company shall retain records of the due diligence process.

19.4 Contractual Arrangements

All material third-party service providers shall be engaged under written agreements.

Where applicable, agreements should address:

- Scope of services.
 - Roles and responsibilities.
 - Confidentiality obligations.
 - Data protection requirements.
 - Information security obligations.
 - Service levels.
 - Compliance with applicable laws.
 - Termination arrangements.
-

19.5 Ongoing Monitoring

The Company shall periodically review the performance of third-party service providers to ensure that services continue to meet operational and regulatory expectations.

Monitoring activities may include:

- Service availability.
- Operational performance.
- Security incidents.
- Customer impact.
- Regulatory compliance.
- Contract performance.
- Review of significant operational issues.

Where deficiencies are identified, appropriate corrective actions shall be taken.

19.6 Information Security

Where third-party service providers have access to Company information or customer data, appropriate security controls shall be implemented.

Such controls may include:

- Confidentiality agreements.
- Access restrictions.
- Secure data transmission.
- Data protection obligations.
- Periodic security reviews.

Third-party providers shall only receive access necessary to perform their contracted services.

19.7 Regulatory Compliance

The Company shall ensure that outsourced services do not compromise its regulatory obligations.

Where required, the Company shall cooperate with regulatory authorities regarding outsourced activities and maintain appropriate records demonstrating oversight of third-party service providers.

19.8 Termination of Third-Party Services

Where a third-party service provider no longer meets the Company's operational, security or compliance requirements, the Company may terminate the service relationship in accordance with the applicable contractual arrangements.

Following termination, the Company shall ensure:

- Company information is returned or securely destroyed where appropriate.
 - Access to Company systems is removed.
 - Outstanding operational matters are resolved.
 - Relevant records are retained.
-

19.9 Reference Documents

This chapter should be read together with:

- Information Security
 - Privacy Policy
 - AML/CFT Policy
 - Business Continuity Management
 - Vendor Agreements
-

19.10 Third-Party Management Workflow

Business Requirement

→ Vendor Selection

→ Due Diligence

→ Contract Approval

→ Service Implementation

→ Performance Monitoring

→ Periodic Review

→ Contract Renewal / Termination

20. Document Control

20.1 Purpose

AG Group B.V. maintains a Document Control process to ensure that all operational policies, procedures and manuals remain accurate, up to date and compliant with applicable legal and regulatory requirements.

The objective of this process is to ensure that only current and approved documents are used within the Company's operations.

20.2 Scope

This chapter applies to all internal operational documents, including but not limited to:

- Operational Manual
 - Terms and Conditions
 - Responsible Gaming Policy
 - AML/CFT Policy
 - Privacy Policy
 - Player Complaints Policy
 - Internal operational procedures
 - Compliance guidelines
 - Business continuity documentation
-

20.3 Document Ownership

Each operational document shall have an assigned document owner responsible for:

- Maintaining the document.
 - Reviewing its contents.
 - Coordinating updates.
 - Ensuring consistency with applicable laws and regulations.
 - Obtaining the necessary approvals before implementation.
-

20.4 Document Review

Operational documents shall be reviewed:

- At least annually.
- Following significant regulatory changes.
- Following major operational changes.
- After significant incidents.
- Whenever management considers an update necessary.

Documents shall be updated promptly whenever revisions are required.

20.5 Version Control

Each controlled document shall contain, where applicable:

- Document title.
- Version number.
- Effective date.
- Revision date.
- Approval date.
- Document owner.
- Approval authority.

Previous versions shall be archived to maintain an appropriate audit trail.

20.6 Document Approval

New documents and material revisions shall be reviewed and approved by authorised management before implementation.

No controlled document shall become effective until the required approval has been obtained.

20.7 Document Distribution

Only the latest approved version of each controlled document shall be made available for operational use.

The Company shall take reasonable steps to prevent the use of obsolete or superseded documents.

Where appropriate, employees shall be informed when significant revisions are issued.

20.8 Record Retention

Historical versions of controlled documents shall be retained in accordance with the Company's Record Retention procedures.

Document revision history shall be maintained for audit and regulatory purposes.

20.9 Reference Documents

This chapter should be read together with:

- Record Retention
 - Internal Controls
 - Regulatory Reporting
 - Business Continuity Management
-

20.10 Document Control Workflow

Document Created

→ Internal Review

→ Management Approval

→ Version Control

→ Publication

→ Periodic Review

→ Revision (if required)

→ Archive Previous Version

21. Risk Management

21.1 Purpose

AG Group B.V. has established a Risk Management framework to identify, assess, monitor and mitigate risks that may affect its business operations, customers, regulatory compliance and financial stability.

The objective of the Risk Management framework is to support sound corporate governance, maintain operational resilience and ensure compliance with applicable legal and regulatory requirements.

21.2 Risk Management Framework

The Company adopts a risk-based approach to managing its business activities.

Risk management is an ongoing process that includes:

- Risk identification.
- Risk assessment.
- Risk mitigation.
- Continuous monitoring.
- Periodic review.

Management is responsible for ensuring that appropriate controls are implemented to reduce risks to an acceptable level.

21.3 Risk Identification

The Company identifies risks arising from its operations on an ongoing basis.

Key risk categories include:

- Operational Risk
- Compliance Risk
- AML/CFT Risk
- Cybersecurity Risk
- Financial Risk
- Third-Party Risk

- Business Continuity Risk
- Reputational Risk

New risks shall be assessed whenever there are significant changes to business operations, regulatory requirements or technology.

21.4 Risk Assessment

Each identified risk is evaluated based on its:

- Likelihood of occurrence.
- Potential operational impact.
- Financial impact.
- Regulatory impact.
- Customer impact.
- Reputational impact.

Management shall determine whether existing controls are adequate or whether additional mitigation measures are required.

21.5 Risk Mitigation

Where risks are identified, appropriate mitigation measures shall be implemented.

Examples include:

- Internal operational controls.
- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD).
- Information security controls.
- Business continuity planning.
- Disaster recovery procedures.
- Staff training and awareness.
- Regular policy reviews.
- Ongoing monitoring of third-party service providers.

The effectiveness of mitigation measures shall be reviewed periodically.

21.6 Risk Monitoring

The Company continuously monitors its operational environment to identify emerging risks and evaluate the effectiveness of existing controls.

Monitoring activities include:

- Operational performance reviews.
- Compliance monitoring.
- AML/CFT monitoring.
- Information security monitoring.
- Customer complaint analysis.
- Incident reporting.
- Regulatory developments.

Significant risks shall be reported to management without undue delay.

21.7 Management Review

Senior management shall periodically review the Company's overall risk profile.

The review includes:

- Emerging operational risks.
- Compliance risks.
- Financial risks.
- Information security risks.
- Business continuity readiness.
- Effectiveness of existing controls.

Where necessary, management shall approve corrective actions and allocate appropriate resources to address identified risks.

21.8 Continuous Improvement

The Company is committed to continuously improving its Risk Management framework.

Risk management procedures shall be reviewed whenever:

- Regulatory requirements change.
- Significant operational changes occur.
- Major incidents are identified.

- New technologies are introduced.
- Internal reviews recommend improvements.

Updates shall be documented and communicated to relevant personnel.

21.9 Reference Documents

This chapter should be read together with:

- AML/CFT Policy
 - Information Security Procedures
 - Business Continuity Management
 - Disaster Recovery Procedures
 - Internal Controls
 - Incident Management
-

21.10 Risk Management Workflow

Risk Identification

→ Risk Assessment

→ Risk Evaluation

→ Risk Mitigation

→ Continuous Monitoring

→ Management Review

→ Continuous Improvement

22. Training and Staff Awareness

22.1 Purpose

AG Group B.V. recognises that competent and well-informed employees are essential to maintaining regulatory compliance, operational integrity and customer protection.

The Company is committed to providing appropriate training and awareness programmes to ensure that employees understand their responsibilities and comply with applicable legal, regulatory and internal policy requirements.

22.2 Scope

This training programme applies to all employees whose duties relate to the Company's operations.

Training requirements are determined based on each employee's role and responsibilities.

Additional or specialised training may be provided where required.

22.3 Induction Training

New employees shall receive induction training before assuming operational responsibilities.

Induction training includes, where applicable:

- Company policies and procedures.
 - Employee responsibilities.
 - Code of conduct.
 - Operational procedures.
 - Customer protection principles.
 - Information security awareness.
 - Data protection requirements.
-

22.4 Compliance Training

Employees whose responsibilities involve regulatory compliance shall receive appropriate compliance training.

Training topics may include:

- Applicable legal and regulatory requirements.
- Internal operational procedures.
- Regulatory reporting obligations.

- Risk management.
 - Internal controls.
-

22.5 AML/CFT Training

Relevant employees shall receive periodic AML/CFT training covering:

- Customer Due Diligence (CDD).
- Enhanced Due Diligence (EDD).
- Suspicious activity identification.
- Transaction monitoring.
- Reporting obligations.
- Record retention requirements.

Employees shall understand their responsibilities for preventing money laundering and terrorist financing.

22.6 Responsible Gaming Training

Employees interacting with customers shall receive Responsible Gaming training.

Training includes:

- Responsible Gaming principles.
 - Recognition of gambling-related harm.
 - Self-exclusion procedures.
 - Customer support responsibilities.
 - Escalation procedures.
-

22.7 Information Security and Data Protection Training

Employees shall receive training on information security and personal data protection.

Training topics include:

- Password security.
- Access control.
- Confidentiality obligations.

- Secure handling of customer information.
 - Phishing awareness.
 - Incident reporting.
 - Data protection requirements.
-

22.8 Refresher Training

The Company shall provide refresher training periodically to ensure employees remain aware of current legal, regulatory and operational requirements.

Additional training may be provided following:

- Regulatory changes.
 - Policy updates.
 - Operational changes.
 - Significant incidents.
 - Introduction of new systems or technologies.
-

22.9 Training Records

The Company maintains records of employee training activities.

Training records may include:

- Training topic.
- Training date.
- Participants.
- Training materials.
- Completion status.

Training records shall be retained in accordance with the Company's Record Retention procedures.

22.10 Management Responsibilities

Management is responsible for ensuring that employees receive appropriate training relevant to their duties.

Management shall periodically review training programmes to ensure they remain effective and aligned with applicable regulatory requirements.

22.11 Reference Documents

This chapter should be read together with:

- AML/CFT Policy
 - Responsible Gaming Policy
 - Privacy Policy
 - Information Security Procedures
 - Internal Controls
-

22.12 Training and Staff Awareness Workflow

Employee Joined

- Induction Training
- Role-specific Training
- AML / Responsible Gaming / Information Security Training
- Daily Operational Responsibilities
- Periodic Refresher Training
- Training Record Maintenance

Version	Date	Description	Approved By
1.0	July 2026	Initial Release	Director