

Information Security Policy

Seven Days B.V.

Applicable to: Weeekly | Weeekly Rivals | Casino

Prepared in alignment with:

National Ordinance on Games of Chance (LOK), 20 December 2024

GCB AML/CFT Regulations, January 2025

Curacao Gaming Authority framework

Version 1.0

Effective Date: [ON LICENCE GRANT]

Issued by: Seven Days B.V.

Curacao Gaming Authority Licence No. [LICENCE NUMBER]

Document Control

Version History

Version 1.0 - Initial draft prepared for review.

Reading Notes

- Section references to the LOK refer to the National Ordinance on Games of Chance dated 20 December 2024.
- References to AML/CFT obligations, CDD thresholds, and UTR reporting refer to the GCB AML/CFT Regulations dated January 2025 and related instruments.
- Where this policy is silent on a specific operational implementation, the relevant standard operating procedure or operations-manual section governs.
- Any apparent conflict between this policy and the LOK, the GCB AML/CFT Regulations, or any binding CGA guidance must be resolved in favour of the regulatory instrument.

1. Purpose and Scope

1.1 Purpose

Seven Days B.V. (“the Company”), a company incorporated under the laws of Curaçao, owns and operates the Platform at weewkly.com. The purpose of this Information Security Policy is to establish a comprehensive framework for protecting the confidentiality, integrity, and availability of all information processed, stored, or transmitted by the Company in connection with the Platform.

In this policy, “the Platform” means the integrated gaming offering available at weewkly.com, comprising the Weewkly prize-pool raffle, Rivals competitive wagering, the Casino, and all third-party game content; references to “Weewkly” mean the raffle product unless the context indicates the wider Platform.

This policy ensures that all data, systems, digital assets, and supporting infrastructure are safeguarded against unauthorised access, misuse, loss, manipulation, or disruption, in alignment with the National Ordinance on Games of Chance (LOK) of 20 December 2024, the GCB AML/CFT Regulations of January 2025, and accepted international information security standards.

The objectives of this policy are to:

- Maintain secure and compliant operations consistent with Curacao Gaming Authority (CGA) standards, AML/CFT obligations, and recognised information security best practices.
- Protect player data, internal data, platform logic, financial records, and the integrity of stablecoin custody arrangements.
- Define consistent security expectations for staff, contractors, and third-party partners to ensure a unified approach across all parties.
- Reduce risk arising from cybersecurity threats, operational failures, internal misuse, or external attacks.
- Support business continuity and secure, uninterrupted gaming operations on the Platform.

1.2 Scope

This policy applies to all information assets, systems, personnel, and third parties engaged in the operation of the Platform.

Covered Platforms

Weekly

- Weekly prize pool raffle.
- Ticket-based entries through bundles and memberships using supported cryptocurrencies.
- Internal Coin-based games and progression mechanics.
- Wallet security, payout logic, and player balance protection.

Rivals

- Competitive wagering format with leaderboard-based outcomes.
- Real-money buy-ins using supported cryptocurrencies with even-start virtual currency wagering.
- Leaderboard logic, and prize allocation mechanisms.
- Wallet security, payout logic, and player balance protection.

Casino

- In-house and third-party casino game content.
- Real-money wagering using supported cryptocurrencies.
- Game integration logic, session handling, and bet/win settlement.
- Wallet security, payout logic, and player balance protection.

1.3 Personnel and Operational Applicability

This policy applies to all individuals who access, manage, or process information assets in connection with the Platform, including:

- Employees and the executive team.
- Contractors and consultants.
- Customer support personnel.
- Developers and engineers.
- Compliance, AML, and risk personnel.
- Marketing and operations staff.

All personnel must comply with the controls, standards, and obligations defined within this document.

1.4 Third-Party Applicability

This policy also applies to all external partners and service providers that store, process, or access the Company's systems or data, including:

- Game suppliers and aggregators.
- Payment processors and crypto custody providers.
- KYC and AML identity verification vendors.
- Blockchain analytics and wallet screening providers.

- Cloud hosting providers and data center operators.
- Security and monitoring service providers.

All third parties must adhere to the Company's minimum security standards, contractual requirements, and data-handling obligations.

1.5 Systems and Data Covered

Systems

- Application servers.
- Web and mobile platforms.
- Admin consoles and back-office dashboards.
- Player account management systems.
- Payment and crypto custody infrastructure.
- Logging, monitoring, and analytics systems.
- Anti-fraud and AML monitoring tools.
- Cloud hosting environments.
- Third-party integrations.

Data Types

- Personally identifiable information (PII), including name, date of birth, email, IP address, and device identifiers.
- Cryptocurrency data, including wallet addresses, deposits, withdrawals, and on-chain analysis.
- Gaming data, including bets, spins, coin usage, leaderboards, and gameplay history.
- Prize-pool, raffle, and competition data.
- Transaction data, including transfers, ticket purchases, and game wagers.
- Operational and internal business data.
- Audit logs and security logs.

1.6 Regulatory Anchors

This policy is designed to support compliance with, among other instruments:

- The National Ordinance on Games of Chance (LOK) of 20 December 2024, including the operations-manual obligations under Article 5.9, the reporting obligations under Article 5.10, the record-keeping obligations under Article 5.11, and the requirement to maintain digital player and transaction records on a Tier-IV certified data center registered in Curacao under Article 5.9(1)(j).
- The GCB AML/CFT Regulations of January 2025, including customer due diligence triggers, enhanced due diligence requirements, transaction reporting through the goAML reporting portal, and the obligation to retain records for a minimum of five years.
- Sanctions obligations arising under the Sanctions National Ordinance and the Kingdom Sanctions Act.

Where this policy refers to specific regulatory articles or thresholds, those references are anchored to the legal instruments in force at the time of the most recent policy review and must be re-validated against current text as part of the annual review cycle.

The control set in this policy is structured around the CGA Information Security Control Requirements, which adopt the CIS Controls Implementation Group 1 (IG1) as the mandatory baseline and align with ISO/IEC 27001:2022. The Company intends to mature its controls toward CIS IG2 over time as the business scales.

1.7 Enforcement

All individuals and third parties under the scope of this policy are required to comply with its standards. Non-compliance may result in disciplinary action, account suspension, vendor termination, or regulatory reporting, depending on severity.

2. Information Security Objectives

The primary objective of this policy is to establish, implement, and maintain a robust security framework that protects the Company's digital assets, gaming systems, player information, and financial infrastructure.

2.1 Confidentiality, Integrity, and Availability

The Company adheres to the internationally recognised confidentiality, integrity, and availability (CIA) model to guide all information security practices.

2.1.1 Confidentiality

Information must be safeguarded from unauthorised access, disclosure, or misuse. This includes ensuring that:

- Player data and personal information remain protected at all times.
- Access to internal systems is strictly controlled via authentication and role-based permissions.
- Sensitive operational data, including admin logs, wallet credentials, and game configuration, is limited to approved personnel.
- Third-party integrations operate under strict data protection agreements.
- Encryption is applied to data both in transit and at rest.

2.1.2 Integrity

All data must remain accurate, consistent, and unaltered except by authorised processes. This includes:

- Preventing tampering, manipulation, or corruption of game outcomes, randomisation, raffle ticket allocations, prize-pool calculations, leaderboard logic, and player balance and transaction records.
- Detecting and blocking fraudulent or automated attempts to alter gameplay or results.
- Maintaining verifiable audit logs of all system changes.

- Implementing secure development, version control, and change management processes.

2.1.3 Availability

Systems, services, and data must be accessible to authorised users when needed. This includes:

- Maintaining stable uptime for raffles, competitions, internal coin mechanics, and all wagering and payment functions.
- Implementing redundant infrastructure, load balancing, and DDoS protection.
- Ensuring reliable access to admin panels, AML tools, monitoring systems, and payment gateways.
- Establishing robust incident responses and business continuity procedures.

2.2 Protection of Player Funds and Crypto Wallets

The Company is committed to protecting all assets related to real-money operations.

Stablecoin Custody Security

- Player-facing deposits and withdrawals are processed in supported regulated stablecoins, currently USDT and USDC, segregated by asset within a regulated custodial infrastructure.
- Multi-signature or multi-party computation (MPC) authorisation is required for material movements.
- Secure storage and access controls for cryptographic credentials.
- Hot wallet float limitations and cold wallet safeguarding.
- Transaction velocity limits and anomaly detection.
- Segregation of operational funds and player balances.

Fraud and AML Protection

- Continuous monitoring using blockchain analytics, including detection of mixer exposure, sanctions exposure, and wallet risk scoring.
- Automated flags for suspicious activity.
- Tiered withdrawal thresholds and enhanced due diligence where required.

These controls ensure players can trust the integrity of deposits, balances, withdrawals, and prize distributions.

2.3 Compliance With Curacao Gaming Authority Requirements

The Company aligns its information security framework with CGA expectations, including:

- Protection of player data and operational systems.
- Internal controls around gaming logic, randomisation, and prize allocation.
- Secure, transparent financial processes for stablecoin deposits and withdrawals.
- Auditability of all transactions, game outcomes, and administrative actions.
- Vendor oversight and secure integration with all third-party providers.
- Policies that support AML/CFT compliance frameworks.
- Timely incident reporting and cooperation with regulators.

- Maintenance of digital player and transaction records on a Tier-IV certified data center registered in Curacao.

2.4 Continuous Improvement

The Company will regularly:

- Review and update this Information Security Policy.
- Conduct internal audits and vulnerability assessments.
- Monitor emerging cyber threats and industry trends.
- Enhance security controls in alignment with recognised standards.
- Review third-party security practices and compliance.

3. Roles and Responsibilities

To ensure effective implementation, monitoring, and enforcement of this policy, the following roles and responsibilities are assigned. These ensure clear accountability, proper segregation of duties, and consistent adherence to security and regulatory requirements.

3.1 Information Security Officer

The Information Security Officer (ISO) oversees development, implementation, and continuous improvement of the security framework.

Responsibilities

- Develop, maintain, and enforce all information security policies and procedures.
- Oversee security controls across infrastructure, applications, and data.
- Monitor overall risk exposure and recommend improvements.
- Coordinate vulnerability assessments, penetration testing, and system hardening.
- Manage access controls, privileged accounts, and authentication standards.
- Lead internal security reviews and compliance monitoring.
- Ensure cryptographic key management meets industry standards.
- Report security-related metrics, risks, and incidents to senior management.
- Ensure staff receive ongoing security training and awareness sessions.

3.2 Compliance Officer

The Compliance Officer is the senior, operationally independent person responsible for AML/CFT and regulatory compliance.

Responsibilities

- Oversee identity verification, KYC, enhanced due diligence (EDD), and source-of-funds and source-of-wealth processes.

- Monitor transactional activity for suspicious behavior using blockchain analytics and AML monitoring systems.
- Review flagged accounts and determine required escalation, investigation, or enforcement actions.
- Manage sanctions screening procedures, including IP checks, wallet-address checks, and geographic restrictions.
- File unusual transaction reports with the FIU through the goAML portal.
- Provide AML and counter-financing of terrorism (CFT) training to relevant staff and business units.
- Maintain comprehensive AML manuals, internal procedures, red-flag indicators, and risk matrices.
- Collaborate with security, fraud, and engineering teams to detect and mitigate suspicious behavior, account compromise, or wallet anomalies.
- Prepare the annual Business Risk Assessment and submit it to the Board for adoption.

3.3 Data Protection Lead

A Data Protection Lead is appointed to oversee handling of player personal data. The role may be held by the ISO or another designated officer.

Responsibilities

- Oversee handling of player PII consistent with applicable data-protection expectations and contractual obligations.
- Monitor the collection, storage, processing, transfer, retention, and deletion of personal data throughout the data lifecycle.
- Manage and respond to user data-rights requests, including access, correction, deletion, and data portability where supported.
- Ensure privacy-by-design and privacy-by-default principles are embedded within all relevant systems, applications, and development processes.
- Conduct data-protection impact assessments where processing activities present elevated privacy or security risks.
- Liaise with regulators, supervisory authorities, and external agencies regarding data-privacy obligations, inquiries, or breaches.

3.4 Technical Leads

Technical leads, including developers, infrastructure engineers, and security engineers, oversee the design, development, deployment, and maintenance of all digital infrastructure across the Platform.

Responsibilities

- Implement secure coding practices and participate in formal code reviews throughout the development lifecycle.
- Maintain server security, cloud configurations, network perimeter controls, and systems-patching schedules.

- Oversee CI/CD pipelines, ensuring strict access controls, code-integrity checks, and secure deployment standards.
- Support encryption practices, secure network architecture, and environment segregation across development, staging, and production.
- Collaborate with the ISO during vulnerability assessments, penetration testing, and remediation planning.
- Maintain version-control governance, rollback strategies, deployment records, and change-management documentation.
- Ensure gaming logic, RNG systems, and prize-allocation algorithms are tamper-resistant and independently verifiable.
- Ensure platform uptime, service redundancy, backup integrity, and disaster-recovery readiness.

3.5 Customer Support Leads

Customer Support Leads ensure player interactions are handled securely and in compliance with operational procedures.

Responsibilities

- Protect player data during interactions and troubleshooting.
- Verify customer identity before sharing account information.
- Escalate suspected fraud, AML concerns, or unusual player behavior.
- Maintain secure handling of support tickets, emails, and chat logs.
- Follow internal procedures for password resets, account access, and disputes.
- Ensure support teams understand and follow information security requirements.

3.6 Vendor Oversight Lead

The Vendor Oversight Lead ensures that all third-party service providers meet the Company's security, compliance, and contractual obligations.

Responsibilities

- Conduct due diligence and risk assessments before onboarding vendors.
- Maintain an updated vendor register with assigned risk categories.
- Ensure third-party agreements include security, confidentiality, and data-protection clauses.
- Review vendor performance, security updates, and audit reports.
- Monitor third-party access to systems and revoke access when no longer required.
- Coordinate with the ISO and Compliance Officer for vendor-related compliance issues.
- Ensure secure integration with game suppliers, KYC vendors, and payment processors.

3.7 Incident Response Lead

The Incident Response Lead coordinates and manages the response to security incidents.

Responsibilities

- Lead the incident response lifecycle: detection, containment, eradication, recovery, and post-incident review.
- Activate escalation protocols and inform senior management when required.
- Coordinate cross-functional teams during security events.
- Ensure evidence is collected, preserved, and logged appropriately.
- Manage communication with regulators, partners, or affected users where necessary.
- Maintain and update the Incident Response Plan.
- Conduct post-incident reviews and ensure lessons learned are implemented.

3.8 Documentation, Accountability, and Auditing

Clear documentation of responsibilities and audits is maintained to ensure accountability across all roles.

Requirements

- Each role must have written responsibilities within internal documentation.
- All privileged actions, including admin console changes, wallet operations, and system configurations, must be logged and auditable.
- Annual internal audits will be conducted to evaluate compliance with this policy.
- Findings and corrective actions must be documented and tracked.
- Evidence of training, access reviews, and compliance checks must be maintained.
- Vendor audits and performance reviews must be stored securely.
- An annual self-assessment of information security controls is completed using the template provided by the CGA, where applicable, and submitted as required.
- An independent third-party security audit is conducted at the cadence required by the CGA for online operators, and the Company cooperates with CGA reviews, inspections, and technical validation, including any unannounced assessments.

4. Risk Management

The Company maintains a risk management framework to identify, assess, treat, and monitor risks affecting the safe, responsible, transparent, verifiable, and reliable offering of Games of Chance, and to satisfy the risk-based obligations under the AML/CFT Regulations.

4.1 Scope of Risk Management

Risk management under this policy covers, at a minimum:

- Information security risks, including cyber threats, unauthorised access, data loss, and infrastructure failure.
- Money laundering, terrorism financing, and proliferation financing risks (ML/TF/PF).
- Operational risks affecting platform availability, payout integrity, raffle and competition fairness, and player fund safekeeping.

- Regulatory and compliance risks, including changes to the LOK, GCB AML/CFT Regulations, sanctions obligations, and other applicable instruments.
- Third-party and supply-chain risks arising from vendors, custodial providers, and game suppliers.
- Player-protection risks, including risks to vulnerable persons and risks of underage participation.

4.2 Business Risk Assessment

The Company conducts an annual Business Risk Assessment as required by the GCB AML/CFT Regulations. The BRA is documented in the AML/CFT Policy and is referenced here for completeness. Risk outputs from the BRA inform the Information Security Risk Assessment in Section 4.3.

4.3 Information Security Risk Assessment

In addition to the BRA, the Information Security Officer conducts an annual information security risk assessment covering the assets, systems, and data described in Section 5 (Asset Inventory and Classification). The information security risk assessment:

- Identifies threats and vulnerabilities applicable to each in-scope asset category.
- Evaluates the likelihood and impact of identified risks.
- Records risks in a Risk Register maintained by the ISO.
- Assigns a risk owner to each entry.
- Defines a treatment decision and a target residual-risk position.
- Is reviewed quarterly and refreshed annually, or sooner following major incidents, infrastructure changes, or new product launches.

4.4 Risk Assessment Methodology

Risks are assessed using a likelihood-by-impact methodology. Each risk is rated on the following scales:

Likelihood

- Rare: not expected to occur in normal operating conditions.
- Unlikely: could occur but is not expected.
- Possible: may occur at some point.
- Likely: expected to occur in normal operating conditions.
- Almost certain: expected to occur frequently.

Impact

- Negligible: minor inconvenience, no regulatory, financial, or reputational impact.
- Minor: limited operational disruption, no material financial loss, no regulatory exposure.
- Moderate: meaningful operational disruption, limited financial loss, possible regulatory inquiry.
- Major: significant operational disruption, material financial loss, regulatory action likely, player harm possible.
- Severe: platform-wide outage, large financial loss, license-affecting regulatory consequences, or significant player harm.

The combined likelihood-and-impact rating determines whether a risk is classified as Low, Medium, High, or Critical. High and Critical risks must be escalated to senior management and require a documented treatment plan.

4.5 Risk Treatment

For each identified risk, one of the following treatment options is selected and documented:

- Mitigate: implement controls to reduce likelihood, impact, or both.
- Transfer: shift the risk through contractual arrangements, insurance, or use of qualified third-party providers.
- Avoid: discontinue or decline the activity, giving rise to the risk.
- Accept: accept the residual risk where the cost of further treatment is disproportionate, with documented justification and senior management approval.

Acceptance of any High or Critical residual risk requires explicit approval from the Board or its delegated authority and must be recorded in the Risk Register with a defined review date.

4.6 Risk Register

The Company maintains a Risk Register that records, for each identified risk, at a minimum:

- Risk identifier and description.
- Risk category (information security, AML/CFT, operational, regulatory, third-party, player protection).
- Inherent likelihood and impact rating.
- Existing controls.
- Residual likelihood and impact rating.
- Treatment decision and treatment plan.
- Risk owner.
- Target review date.

The Risk Register is maintained by the ISO, with input from the Compliance Officer for AML/CFT entries. It is reviewed at least quarterly and updated whenever a material risk event occurs.

4.7 Risk Monitoring and Reporting

Risk exposure is monitored through:

- Continuous monitoring of security, AML, and operational alerts as described in Section 12 (Logging, Monitoring, and Alerting).
- Quarterly review of the Risk Register by the ISO and the Compliance Officer.
- Annual reporting to the Board, including a summary of the BRA, information security risk position, top risks, and treatment progress.
- Ad-hoc reporting to senior management following any High or Critical risk event.

4.8 Linkage to Other Policies and Controls

Risk management outputs feed directly into:

- The AML/CFT Program, including CDD/EDD triggers, transaction monitoring thresholds, and sanctions screening calibration.
- The asset classification framework in Section 5.
- The access control framework in Section 6.
- The third-party due diligence framework in Section 8.
- The BCDR objectives in Section 14.
- The training program in Section 16.

This ensures that controls implemented under this policy are calibrated to the risks identified through the assessment process, rather than applied uniformly without reference to risk.

5. Asset Inventory and Classification

A structured and comprehensive inventory of all information assets is maintained to ensure appropriate protection based on sensitivity, regulatory obligations, and operational risk. Every asset, whether data, software, hardware, or third-party integration, is classified, monitored, and safeguarded according to this policy.

5.1 Asset Inventory Overview

A centralised Information Asset Register (IAR) is maintained by the ISO. The register includes:

- Asset type and description.
- Owner or responsible department.
- Sensitivity classification.
- Storage location, including the Tier-IV Curacao data center where the asset comprises digital records.
- Applicable controls and encryption requirements.
- Access rights and authorised users.
- Third party involvement, if any.
- Retention periods and backup requirements.
- Change history and versioning, where applicable.

5.2 Asset Categories

The following categories represent the core information assets covered by this policy. Each must be logged, maintained, and protected under defined classification rules.

5.2.1 Player Accounts and Personally Identifiable Information

- Level 1 KYC data captured at signup: name, date of birth, address, and PEP and sanctions screening results.

- Level 2 KYC data captured upon trigger event: identity documents and biometric verification artefacts. These items are classified as Highly Confidential under Section 5.3.4.
- Email addresses and device fingerprints.
- IP addresses, and geographic data.
- Login credentials and authentication information.
- Player behavioral patterns and game history.

5.2.2 Wallet Addresses and Blockchain Transaction Data

- Player deposit addresses.
- Withdrawal addresses.
- Internal hot and cold wallet addresses.
- On-chain activity logs.
- AML screening results, including risk scores, sanctions flags, and mixer alerts.

5.2.3 Game Logic, Algorithms, and RNG Systems

- Game configuration across all platform products.
- In-house RNG used in proprietary games.
- Logic for the Rivals leaderboard.
- Logic for the Weeekly raffle draw mechanism
- Cryptographic seed generation, storage, and rotation for all RNG-dependent systems.
- Provably fair commitment scheme for in-house games across Weeekly, Rivals, and Casino.
- Prize algorithms and payout logic.
- Game outcome logging, audit trail integrity, and reproducibility controls.

5.2.4 Prize Pool Management and Distribution Systems

- Prize pool funding flows.
- Prize pool balance tracking.
- Distribution logic from the prize pool to winning players.
- Automated systems executing weekly draws.
- Audit logs of prize pool changes.

5.2.5 Backend Servers and Administrative Systems

- Admin consoles.
- Customer support dashboards.
- CRM and user account management tools.
- Developer consoles and configuration environments.
- IP allowlists and privileged access systems.

5.2.6 Internal Communication Systems

- Email systems.
- Internal messaging and collaboration platforms.
- Knowledge bases and internal documentation.

- Support communications and ticketing tools.

5.2.7 Third-Party Integrations

- Game-provider APIs.
- KYC and AML vendors.
- Blockchain monitoring tools.
- Payment processors and stablecoin gateways.
- Analytics and behavioral risk systems.

5.2.8 Crypto Custody Systems

- Hot wallet infrastructure.
- Cold wallet storage.
- Multi-signature or MPC structures.
- Key management systems.
- Withdrawal queue logic and automated risk screening.

5.2.9 Monitoring Tools, Logs, and AML Systems

- Server and application logs.
- Transaction logs.
- Security alerts and anomaly detection systems.
- Blockchain analytics tooling.
- Behavioral analysis and fraud detection modules.
- System health metrics, uptime monitors, and performance dashboards.

5.3 Data Classification Levels

To ensure security controls are proportional to sensitivity and risk, four levels of data classification are defined.

5.3.1 Public

Information intended for public distribution.

Examples

- Marketing material.
- Public FAQ content.
- Promotional content.
- Public-facing terms and conditions.

Required Controls

- No special access restrictions.
- Integrity and availability protections are maintained.

5.3.2 Internal

Information intended for internal operational use but not harmful if disclosed.

Examples

- Operational guidelines.
- Low-sensitivity business analytics.
- Non-sensitive internal communications.

Required Controls

- Access restricted to relevant staff.
- Stored on secure internal platforms.

5.3.3 Confidential

Information that could cause operational or reputational harm if exposed.

Examples

- Player account details and PII.
- Staff information.
- Support ticket data.
- Non-public business strategies.
- Game configuration settings.

Required Controls

- Encrypted storage and transmission.
- Role-based access control (RBAC).
- Logging of access events.

5.3.4 Highly Confidential

Information that could cause severe financial, regulatory, or security impact if exposed.

Examples

- Cryptographic credentials and key material.
- Admin-panel credentials.
- Hot-wallet operational logic.
- Source code for core game logic and RNG systems.
- Prize-pool scripts and draw mechanisms.
- AML flags, risk scores, and sanctions findings.
- Level 2 KYC artefacts, including identity documents and biometric verification results.
- Source-of-funds and enhanced due diligence documentation.
- Internal audit trails and privileged-action logs.

Required Controls

- Strict role-based access control with minimum-necessary access.

- Multi-factor authentication.
- Hardware security modules or encrypted vault storage.
- Continuous monitoring and access logging.
- Segregation from general systems.
- Limited internal distribution on a need-to-know basis.

5.4 Asset Ownership and Accountability

Each information asset must have an assigned owner responsible for:

- Ensuring correct classification.
- Approving access requests.
- Documenting changes.
- Ensuring backups and retention comply with policy.
- Coordinating with the ISO for periodic reviews.

5.5 Review and Audit Requirements

- Hardware and infrastructure inventories are reviewed at least twice annually; software, third-party integration, and data inventories at least annually; in each case sooner following major platform changes. Vendor support status for approved software is checked at least monthly, with unsupported software removed or retained only under a documented risk acceptance with compensating controls.
- Highly Confidential assets must be reviewed every quarter.
- Logs and documentation must be accessible for inspection by the ISO, Compliance Officer, or regulatory authorities.
- Any asset lacking a documented owner or classification must be flagged for immediate review.

6. Access Control Policy

This Access Control Policy ensures that all systems, data, and administrative environments are protected through strict authorisation, consistent authentication, and continuous monitoring of privileged activity. It applies to all employees, contractors, developers, administrators, vendors, and any third-party accessing Company systems.

6.1 Access Control Principles

6.1.1 Role-Based Access Control

All access rights must be assigned based on defined roles rather than individuals and must align with the responsibilities of each role. Examples include:

- Customer support: ticketing system access only.
- Developers: staging environment and code repositories.
- Security and technical leads: production access with limited privileges.

- AML and Compliance: transaction dashboards and risk engines.
- Finance and admin: withdrawal-approval workflows only.

6.1.2 Minimum Privilege

Users must be granted only the minimum level of access necessary to perform their tasks. No user should hold elevated permissions without documented justification. This principle applies to:

- Backend consoles.
- Wallet controls.
- Prize-pool systems.
- Draw management.
- Script execution.

6.1.3 Need-to-Know Basis

Access to sensitive or confidential information must be restricted to individuals with a legitimate operational requirement. Examples:

- Wallet addresses: AML and Finance teams only.
- Player KYC documents: Compliance only.
- Game logic: technical leads only.
- Admin logs: ISO and Compliance Officer only.

6.1.4 Multi-Factor Authentication

Multi-factor authentication is mandatory for all privileged accounts. Specific MFA requirements, acceptable factor types, and fallback rules are set out in Section 7.2.

6.1.5 Separation of Privileged and Standard Accounts

Personnel with privileged access hold separate administrative accounts used only for elevated functions. Privileged accounts are not used for general activity such as email, web browsing, or document editing, which are performed on standard non-privileged accounts.

6.2 Administrative Access Rules

6.2.1 Prize-Pool Systems

Access restricted to

- Information Security Officer.
- Technical Lead.
- Finance or admin personnel for oversight only, not configuration.

Controls

- Read and write access limited to authorised personnel.
- Automated logs of all prize-pool adjustments.
- No manual script execution unless approved and logged.

6.2.2 Crypto Wallet Systems

This includes hot wallets, cold wallets, multi-signature or MPC infrastructure, and the withdrawal queue.

Access restricted to

- Compliance Officer for monitoring purposes.
- Finance Lead.
- Pre-approved senior management.
- Technical Lead for system maintenance only, with no transfer authority.

Controls

- All wallet-related actions require MFA.
- High-value withdrawals require multi-signature or multi-party approval.
- Automated anomaly detection must monitor unusual behavior.

6.2.3 Transaction Processing Systems

Access restricted to

- Finance team.
- Compliance and AML team.
- Information Security Officer.
- Restricted technical staff with documented need.

Controls

- Hard limits on manual adjustments.
- Withdrawals above defined thresholds require human approval.
- Sanctions and AML checks must run automatically before transferring.
- Transaction logs must be immutable and reviewable.

6.2.4 Game Configuration Systems

This includes game-provider configurations, internal game logic, prize algorithms and rulesets, and RNG-related components.

Access restricted to

- Technical leads.
- ISO for oversight.
- Developers, restricted to staging unless production access is explicitly approved.

Controls

- All production changes must follow change management procedures.
- No live-game parameter changes without documented authorisation.
- Audit logs must capture each modification.

6.2.5 Backend Console and Admin Panels

This includes the CRM, user-management console, support dashboards, analytics dashboards, and back-office monitoring tools.

Access restricted by role-based permission groups

- Support: limited view only.
- Compliance: high-level financial and identity data.
- Security: logs and system visibility.
- Admin: highest privilege with strict need-to-know limitation.

Controls

- All privileged accounts must use MFA.
- Session timeout enforced.
- Automated alerts for unusual admin behavior.

6.3 Privileged Action Monitoring and Auditability

All privileged actions must be logged, monitored, and auditable.

Logged

- System configuration changes.
- Wallet access attempts.
- Withdrawal approvals.
- Prize pool updates.
- Admin-panel access.
- Suspended or locked account actions.
- Login failures, password resets, and MFA changes.

Monitored

- Real-time monitoring through Security Information and Event Management (SIEM) tooling.
- Alerts for deviation from normal behavioral patterns.
- Special attention to wallet-related activities.

Auditable

- Logs must be tamper resistant.
- Logs must be retained according to the retention schedule in Section 15.
- Logs must be accessible to ISO, Compliance Officer, and regulatory requests.
- Logs must be reviewed at least quarterly.

Any suspicious privileged activity must trigger immediate investigation.

6.4 Access Review and Revocation

- Access rights and account inventories, covering standard user accounts, privileged administrative accounts, and system or service accounts, are reviewed at least quarterly, and promptly on role change or termination.
- Users leaving the organisation must have all access removed within 24 hours.
- Vendor and contractor access must have expiry dates and limited permissions.
- Stale or unused internal accounts must be automatically disabled after 45 days of non-use, with reactivation requiring documented approval; audit logs are retained on disabled accounts rather than deleted.

6.5 Access Granting Process

Access is provisioned through a documented request that is approved by the relevant manager or resource owner before access is granted, with the granted permissions recorded against the user account. Where a role requires Key Person or other regulated status under the LOK, that status is verified as part of the access workflow and at each access review.

7. Authentication and Password Requirements

Strong authentication controls are essential to protecting the Company's systems, player data, crypto custody arrangements, and administrative tools. The requirements in this section apply to all employees, contractors, vendors, and systems interacting with the Platform.

7.1 Password Complexity Requirements

Minimum Standards

- Minimum length of 12 characters.
- Must contain uppercase letters, lowercase letters, numbers, and special characters.
- Must not contain easily guessable information such as names, dates, or words related to the Company or the user's role.
- Must be unique per system; password reuse is prohibited.

Password Storage Requirements

- All passwords must be hashed using industry-accepted algorithms.
- No plaintext or reversible encryption storage is permitted.
- Password hints must not reveal information about the password structure.

Password Rotation

- Forced rotation is triggered immediately on suspected breach, account compromise, password sharing, or staff departure where credentials may have been known.
- Passwords must not repeat any of the last five previously used passwords.
- Service accounts and shared credentials are rotated quarterly and on staff departure.

7.2 Multi-Factor Authentication Requirements

MFA is mandatory for all staff and all privileged accounts.

MFA Applies To

- Admin panels.
- Prize-pool systems.
- Crypto custody systems, including hot and cold wallet access.
- Customer management and CRM dashboards.
- Withdrawal processing systems.
- Cloud hosting accounts.
- Source code repositories and CI/CD pipelines.
- Payment, KYC, and AML tools.
- Monitoring and SIEM platforms.

Accepted MFA Methods

- Authenticator apps.
- Hardware security keys, preferred for wallet and production access.
- SMS or email MFA only as a backup when hardware-based or app-based MFA is unavailable.

MFA Enforcement

- MFA must be activated during onboarding.
- Users cannot disable MFA without security approval.
- Re-authentication is required for high-risk actions, accessing Highly Confidential data, or adjusting system configurations.

7.3 Session Management and Timeout Rules

Session Timeout Rules

- Admin and privileged dashboards: automatic logout after a short inactivity period.
- Customer support and CRM systems: logout after a defined inactivity period appropriate to support workflow.
- Backend developer consoles: logout after a short inactivity period.
- Wallet and financial panels: strict inactivity timeout, shorter than other system tiers given the sensitivity.

Forced Session Controls

- Sessions must expire automatically after a maximum lifetime, even if active.
- Concurrent admin sessions are prohibited unless explicitly justified.
- Re-authentication is required when a session reaches a sensitive area.

Session Encryption

- All sessions must use secure cookies.
- Tokens must expire immediately upon logout.

- Session data must not be stored in local browsers beyond one session.

7.4 API Key and Service Credential Security

API keys are sensitive authentication assets and must be protected accordingly.

Storage and Encryption

- API keys must be stored in approved secure-vault solutions.
- Keys must never be stored in source code, logs, frontend applications, emails, or chat messages.
- Encryption must meet AES-256 or equivalent standards for at-rest storage.

API Key Rotation

- Immediate rotation when a developer leaves, on breach or suspected compromise, or if a key is exposed in logs, repositories, or communication channels.

Access Control

- API key access must follow role-based access control, least privilege, and need-to-know justification.
- Access logs must record who accessed the key, when it was accessed, and what it was used for.

Restrictions

- API keys must be scoped to minimum privileges, with read-only and write privileges separated.
- Keys must be environment-specific across development, staging, and production.
- Production keys must never be used in development environments.

7.5 Account Lockout and Failed Login Attempts

- After a number of failed login attempts, the account is temporarily locked.
- Admin accounts lock for an extended period or require manual unlock by the ISO.
- Standard user accounts lock for a reasonable period before automatic unlock.
- Lockout events must generate automatic alerts for monitoring.

7.6 Credential Sharing and Prohibited Practices

The following are strictly prohibited:

- Sharing passwords between staff members.
- Reusing passwords across systems.
- Storing credentials in unsecured files, spreadsheets, or chat platforms.
- Using personal accounts for work-related access.
- Using outdated or weak authentication applications.
- Hardcoding credentials into scripts or code repositories.

Any violation will trigger an investigation and may result in disciplinary action.

7.7 Offboarding and Credential Deactivation

Upon employee departure or role change:

- All accounts must be revoked within 24 hours.
- API keys associated with the user or team must be rotated.
- Access to cloud, infrastructure, CRM, wallet systems, and support tools must be immediately terminated.
- Logs must be reviewed to confirm there was no unauthorised activity prior to termination.

8. Third-Party and Vendor Security

The Company relies on third-party service providers, including game aggregators, KYC vendors, payment processors, custodial infrastructure providers, cloud-hosting platforms, and blockchain analytics tools. Third-party risk is managed using a risk-based approach. The depth of due diligence, contractual controls, and ongoing monitoring is proportionate to the vendor's access to Company systems, the sensitivity of data handled, and the criticality of the service to gaming operations and regulatory compliance.

8.1 Vendor Due Diligence

Before onboarding any third-party provider, the Company must conduct a risk assessment to verify the vendor's security posture and regulatory suitability.

Vendors cannot be approved without a completed due-diligence assessment signed by the Vendor Oversight Lead, the ISO, and the Compliance Officer where relevant.

8.2 Contractual Security Obligations

Vendor agreements must include security and confidentiality obligations appropriate to the vendor's risk rating and the nature of the services provided. Where a vendor is classified as high-risk or has access to Confidential or Highly Confidential data, the agreement must include (or be supplemented by) stronger controls as set out below.

- Clear allocation of security responsibilities, access permissions, and restrictions on data use.
- Data protection obligations for any personal, financial, gaming, or operational data processed on behalf of the Company.
- Secure data transmission requirements.
- Encryption and key-management requirements for data at rest, where the vendor stores or caches Company data.
- Incident and breach notification obligations, including prompt notification where the vendor becomes aware of a security incident that may affect Company systems or data.
- Alignment with the Company's security requirements relevant to the service.
- Appropriate remedies for security failures proportionate to the service risk.
- Controls over subcontracting and sub-processors.
- Compliance with applicable laws and regulatory expectations relevant to the service.

- Security assurance rights appropriate to vendor size and risk.

8.3 Data Handling Agreements

Vendors that process player data, financial data, or operational logs must enter into a Data Handling Agreement specifying:

- What data is collected.
- Purpose of processing.
- Storage location and retention period.
- Security controls applied.
- Data minimisation requirements.
- Restrictions on transferring data to third parties.
- Procedures for data deletion or anonymisation.
- Requirements for handling user requests, including access, deletion, and correction.
- Secure disposal of data at the end of the contract.

The agreement must be signed before any data exchange occurs.

8.4 Vendor Access Control Requirements

Access Restrictions

- Vendors may only access systems necessary for their operational function.
- Access must be role-based, time-limited, logged and monitored, and removed immediately when no longer required.
- Vendor accounts must use MFA, unique credentials with no shared logins, and secure VPN or IP-allowlisted connections where required.

Vendors must not access prize-pool logic, crypto custody systems, player balances, internal AML tools, or any Highly Confidential data unless (a) such access is necessary for the contracted service, and (b) it is explicitly approved in advance by the ISO (and Compliance where relevant), documented, time-bound, and protected by compensating controls.

Remote Access

- Remote vendor access must be approved by the ISO.
- Sessions must be logged.
- Actions must be monitored in real time for high-risk systems.

8.5 Ongoing Monitoring and Performance Review

Monitoring Requirements

- Review vendor security reports, audit reports, or certifications annually.
- Monitor vendor performance and reliability metrics.
- Conduct annual vendor risk assessments.
- Confirm vendors maintain secure data storage, encryption standards, incident-response readiness, and uptime commitments.

- Evaluate real-world behaviour, including promptness in resolving issues, transparency, and response to incidents or service outages.

Security Events

If a vendor experiences a breach:

- The vendor must notify the Company without undue delay and within the timeframe agreed contractually once it becomes aware of an incident that may affect Company systems or data.
- The vendor must provide a written incident report containing, at a minimum, scope, suspected root cause, impacted data/systems, mitigation actions taken, and planned remediation and timelines.
- Access to systems may be suspended until risk is mitigated.
- An internal review must be conducted to evaluate impact.

8.6 Vendor Termination and Offboarding

Termination Requirements

- All access credentials must be revoked immediately.
- API keys must be regenerated.
- VPN and IP-allowlist rules must be removed.
- All Company data must be returned securely or destroyed with written proof.
- Data disposal must comply with retention policies, AML/CFT record-keeping obligations, and regulatory reporting rules.

Final Audit

A closing review must confirm that access has been removed, data has been returned or securely destroyed, and any ongoing obligations are documented. The depth of the closing review and required sign-off is proportionate to vendor risk and may include the Vendor Oversight Lead and ISO, with Legal or Compliance involvement where relevant.

8.7 Prohibited Vendor Practices

Vendors may not:

- Store the Company's production data on personal devices or unsecured servers.
- Subcontract tasks without written approval.
- Lower encryption standards or modify security controls without consultation.
- Access systems without MFA.
- Share accounts among team members.
- Retain data after contract termination.
- Use the Company's data for analytics, training, or any purpose beyond contractual obligations.

Violation of any of these terms will result in suspension or termination of access.

8.8 Game Content and Data Feed Integrity

Where the Platform integrates game content, aggregated content, or third-party data feeds used to determine outcomes, those feeds are received over authenticated, encrypted channels and validated for integrity using signatures, hashing, or equivalent. Feed availability and consistency are monitored, and affected offerings are suspended where integrity cannot be assured until it is re-established. Provider contracts include security, incident-notification, and integrity obligations. If sports betting markets are offered in future, live event data feeds are subject to enhanced monitoring given their direct effect on wager outcomes.

8.9 B2B Provider Certification Monitoring

For B2B providers supplying game content, RGS, RNG, or game engines, the Company verifies the provider's CGA licence and required certifications at onboarding and at least annually, with evidence retained in the Information Asset Register. Contracts require the provider to maintain valid certifications and notify the Company of any change. Where a required certification lapses or is withdrawn, the Company ceases offering affected content until it is restored and notifies the CGA.

9. Network and Infrastructure Security

A secure, resilient, and monitored infrastructure is maintained to protect platform integrity, ensure stable uptime, and safeguard player and operational data. These controls apply to all cloud environments, servers, APIs, backend consoles, third-party integrations, and network components, with specific reference to the Tier-IV Curacao data center for digital records of players, gaming transactions, and financial transactions.

9.1 Curacao Tier-IV Data Centre

The Company maintains digital records of specific critical information about players, their gaming transactions, and their financial transactions on a server hosted within a Tier-IV certified data center registered in Curacao. These records must always be available to the CGA.

Operational requirements include:

- Records covered by LOK Article 5.9(1)(j) are stored on infrastructure located within a Curacao-registered Tier-IV certified data centre.
- Replication, redundancy, and disaster-recovery arrangements must not result in the in-scope records being held only outside the Curacao Tier-IV facility.
- Direct, read-level access for the CGA must be supportable, including the ability to provide records within the timeframes specified by the CGA.
- Where supplementary data is hosted in other regions for performance, redundancy, or analytics purposes, the in-scope record set held in the Curacao Tier-IV facility must remain authoritative and complete.
- Data-centre certification, audit reports, and registration evidence must be retained as part of the Information Asset Register.

9.2 Secure Coding Practices

A secure software development lifecycle (SDLC) is followed to prevent vulnerabilities in all platform components.

Requirements

- All developers must follow OWASP Top 10 and applicable SEI CERT coding guidelines.
- Code must undergo peer review, static application security testing (SAST), and dynamic application security testing (DAST).
- Secrets, credentials, and API keys must never be stored in code repositories.
- Use of environment variables and secure vaults is mandatory.
- Dependencies must be monitored and updated regularly using dependency-scanning tools.
- Production code changes require change-management approval, version control, and deployment logs.
- High-risk components, including RNG, prize-pool algorithms, and wallet interfaces, must undergo enhanced review.

9.3 Firewalls and Network Protection

Firewall Controls

- Network firewalls must be configured to restrict inbound and outbound traffic based on least privilege.
- IP allowlisting required for administrative access.
- Database servers must not be directly exposed to the internet.
- Firewall-rule reviews must be conducted at least quarterly.
- Connections to administrative interfaces, VPN, and privileged-access systems are continuously logged, with automated alerting on unrecognised or unmanaged devices; detected devices are blocked or removed and the action is logged. These connection logs are reviewed under a documented procedure at least weekly to confirm alerting is functioning and to identify any anomalies.

Web Application Firewall

A web application firewall (WAF) must be deployed to protect web applications against:

- SQL injection.
- Cross-site scripting (XSS).
- Cross-site request forgery (CSRF).
- API abuse.
- Known vulnerability exploits.

WAF logs must integrate into central monitoring systems for real-time alerting.

9.4 Distributed Denial-of-Service Mitigation

Requirements

- Use of cloud-based DDoS mitigation services.

- Automated rate limiting on API endpoints.
- Traffic anomaly detection and auto-blocking mechanisms.
- Redundant infrastructure to maintain availability during attacks.

Mitigation tooling must be monitored continuously, and response strategies documented within the Incident Response Plan.

9.5 Encryption Standards

9.5.1 Data in Transit

- All data transmitted across public or internal networks must use TLS 1.2 or TLS 1.3.
- Certificates must be rotated prior to expiration.
- Insecure protocols including HTTP, FTP, and Telnet are prohibited.

9.5.2 Data at Rest

- All sensitive data must be encrypted using AES-256 or stronger.
- Encryption must apply to database storage, backups, logs containing PII, hot-wallet infrastructure, and API secrets and access tokens.

9.5.3 Key Management

- Encryption keys must be stored in hardware security modules (HSMs) or approved cloud key-management services.
- Key rotation must occur every 12 months or upon suspected compromise.
- Access to keys must follow role-based controls and require MFA.

9.6 Environment Segmentation and Isolation

9.6.1 Environment Definitions

- Production: live player platform and operational systems.
- Staging: pre-production testing environment.
- Development: code development and non-sensitive testing environment.

Rules and Restrictions

- Production access is limited to approved senior technical staff.
- Staging and development environments must not contain any production data.
- Synthetic or anonymised test data must be used for all development and testing.
- Network and database segregation must prevent lateral movement between environments.
- CI/CD pipelines must enforce environment-specific credentials.

9.7 Infrastructure Hardening

Requirements

- Disable unused ports and services; disable, rename, or secure default accounts and change all default passwords on deployment.

- Patching of operating systems, databases, application frameworks, libraries, and dependencies at least monthly, with critical security patches applied within the timelines in Section 10.7. Workforce browsers and email clients are kept on supported, current versions.
- Enforce secure configurations for web servers, database servers, and containerised applications.
- Centrally managed anti-malware or endpoint protection on corporate endpoints and supported servers, with automatic updates and regular scanning.
- Maintain documented hardening standards per asset class based on vendor baselines or CIS Benchmarks, stored as configuration baselines and reviewed at least annually.
- Host-based firewalls enabled on servers and supported endpoints with default-deny rules and allow-listing for required services.
- Network infrastructure firmware and software currency reviewed at least monthly; end-of-life products are not used in live environments.
- DNS filtering deployed on corporate endpoints, including remote workers, using a managed provider with updated threat intelligence to block known malicious domains, configured not to disrupt legitimate gaming, custody, or cloud services.
- Removable media is disabled by default, with autorun and autoplay turned off; any approved use requires ISO authorisation and an encrypted device, and is never permitted on devices used for wallet operations or transaction signing.

9.8 Logging and Monitoring of System Activity

Logging Requirements

Logs must be generated for:

- Login attempts, both successful and failed.
- Privileged account actions.
- Wallet operations.
- Prize-pool modifications.
- Withdrawal processing.
- API requests.
- Firewall and WAF events.
- Application errors and crashes.
- System and infrastructure changes.

Retention and Protection

- Logs must be tamper-proof and stored in secure locations.
- Logs must be retained according to the data retention schedule in Section 15, taking into account the AML/CFT minimum five-year retention obligation for AML-related records.
- Logs containing sensitive data must be encrypted.
- In-scope records must be held on the Curacao Tier-IV server.

Real-Time Monitoring

- Logs must be fed into a Security Information and Event Management (SIEM) platform.

- Automated alerts must be triggered for unusual admin actions, suspicious API behavior, DDoS indicators, wallet anomalies, and high-risk access attempts.

Monitoring is conducted continuously through automated systems that generate alerts, with personnel review during business hours and defined response procedures for alerts raised outside those hours.

9.9 Network Redundancy and High Availability

- Use load balancing and failover mechanisms.
- Maintain redundant cloud regions or availability zones, in accordance with the data-residency requirements set out in Section 9.1.
- Implement automated backups and restoration testing.
- Ensure database replication, real-time, or near real-time.
- Maintain high availability for core systems through redundancy, load balancing, and failover mechanisms.

9.10 Periodic Reviews and Penetration Testing

- Conduct independent external penetration testing at least annually, supplemented by internal testing where resources permit.
- Run vulnerability scans monthly, or continuously through automated tooling.

Identified vulnerabilities are addressed in accordance with the severity-based timelines set out in Section 10.7 of this policy.

- Results must be documented and reviewed by the ISO and the senior technical lead.

10. Application and Game Security

The Company is committed to ensuring the security, fairness, and integrity of all gaming applications on the Platform. This section outlines the controls required to prevent manipulation, maintain game fairness, and protect against cyber threats affecting application layers. These controls apply to internally developed systems and third-party game providers.

10.1 RNG Integrity Protection

Random number generators must be secure, unbiased, and protected from tampering.

Requirements

- RNG implementations must be certified by an approved testing laboratory where applicable.
- Third-party RNG systems must provide certification annually.
- RNG configuration parameters must be locked behind admin permission layers, encrypted, and logged when accessed.
- No developer or staff member may modify RNG behavior in the production environment.
- Any manual override or emergency intervention must be logged and reviewed.

10.2 Game Tampering and Manipulation Prevention

Applications, both internal and third-party, must be protected from malicious interference.

Core Protections

- Code obfuscation for client-side logic to prevent reverse engineering.
- Server-authoritative game outcomes; the client cannot decide outcomes.
- Checksums or signatures to validate data integrity.
- Anti-automation measures to prevent botting or unfair play.
- Input validation to block injection attacks, including SQL, command, template, and code injection.
- Replay-attack protection using unique transaction identifiers.
- Secure WebSocket and API communications.
- Anti-multi-accounting checks.
- Coin and stablecoin outcomes must be validated server-side.
- Leaderboard calculations for the Rivals platform must be locked to backend computation.

10.3 Reverse Engineering and Unauthorised Modification Protection

- Application binaries must be hardened against reverse engineering and decompilation.
- Sensitive application logic must remain server-side.
- Debugging features must be disabled in production builds.
- Unused code paths must be removed before deployment.
- Certificate pinning must be implemented in mobile and web apps where relevant.
- Modification of client traffic must be prevented through TLS enforcement, HSTS, and strict CORS policies.

No production API may be accessible without authentication and authorisation.

10.4 Secure API Integration

All integrations with third-party game providers, payment systems, or operational tools must adhere to strong API security requirements.

API Security Controls

- Encrypted communication via TLS 1.2 or 1.3.
- IP allowlisting for inbound and outbound calls.
- API key protection using secure-vault storage.
- Strict role-based access control for API credentials.
- Rate limiting to prevent abuse.
- Signature verification for incoming provider callbacks.

Game Provider Integration Requirements

- Webhooks and API endpoints must be used only through secure channels.
- Provider payloads must be validated for authenticity and structure.

- Response anomalies and unexpected patterns must be monitored.
- All API requests and responses must be logged in tamper-resistant logs.

10.5 Code Review and Development Controls

Mandatory Code Review Requirements

- Peer review of all code before merging.
- Security checkpoints during development.
- Specialized review for critical systems including wallets, game logic, and prize systems.
- Use of automated scanning tools to detect vulnerabilities.

Developer Access Rules

- Developers may not access production databases or live data.
- Sensitive configuration data must be masked during development.
- Only senior engineers may approve production releases.

10.6 Continuous Integration/Continuous Deployment Pipeline Security

Controls

- MFA required for access to CI/CD tooling.
- Separate pipelines for development, staging, and production.
- No secrets stored in pipelines; all secrets must come from encrypted vaults.
- Automated tests and scans must run before deployment.
- Manual approval is required for any production deployment.
- Deployment logs must be retained and audited.
- Pipeline tooling must be monitored for unauthorised job executions, unexpected configuration changes, and credential access.

Compromises in CI/CD are treated as critical incidents.

10.7 Penetration Testing and Vulnerability Assessments

Penetration Testing Schedule

- External penetration testing at least annually.
- Internal penetration testing after major releases where resources permit.
- API-specific penetration testing for game logic, wallets, and prize-pool systems.
- Mobile and web application penetration tests where applicable.

Vulnerability Scanning

- Automated scans must run weekly for staging and daily or continuously for production.
- Critical vulnerabilities are prioritised for immediate remediation.
- High-severity vulnerabilities are addressed promptly, within a remediation window appropriate to operational risk.
- Medium-severity vulnerabilities are scheduled for remediation within the standard patch cycle.

- Low-severity vulnerabilities are addressed at the next planned maintenance cycle.

Results must be logged, risk-scored, and reviewed by the ISO.

10.8 Anti-Fraud and Gameplay Integrity Measures

Consistent with expectations, the Company deploys fraud-detection and gameplay-integrity mechanisms.

Anti-Fraud Controls

- Real-time monitoring for suspicious betting patterns.
- Player behavior anomaly models, machine-learning-based or rule-based.
- Detection of multiple accounts from the same identity, VPN or proxy abuse, device-fingerprint mismatches, and abnormal win patterns.
- Transaction risk scoring.
- Automated freezing of flagged accounts.

Gameplay Integrity

- Regular audit of leaderboard fairness for the Rivals platform.
- Regular audit of Weeekly raffle draw fairness, including verification of ticket allocation.
- Regular audit of in-house game fairness.
- Verification of game outcomes via server-side logs.
- Alerts for improbable outcomes or impossible win streaks.
- Integrity checks on bonus exploitation and abuse patterns.

These measures must be integrated into the AML and compliance framework.

10.9 Application Logging and Audit Trails

Logs Must Capture

- Every gameplay result.
- All API requests and responses.
- Admin interactions with game settings.
- Prize-pool actions.
- Fraud alerts and anomaly detections.
- Errors, warnings, and unexpected behaviors.

Log Requirements

- Logs must be tamper resistant.
- Logs containing PII or financial data must be encrypted.
- Retention period must meet regulatory requirements as set out in Section 15.
- Logs must be accessible to the ISO, Compliance Officer, and regulators.

11. Crypto and Financial Security Controls

Strict crypto-asset controls are implemented to ensure the security, integrity, and regulatory compliance of all transactions. These controls protect player funds, prevent unauthorised transactions, and support compliance with CGA requirements and global AML/CFT standards. They apply to the management of all digital assets associated with the Platform, including deposits, withdrawals, prize distributions, custody infrastructure, and internal fund movements.

11.1 Wallet Management

11.1.1 Hot and Cold Wallet Separation

- Hot wallets are used exclusively for real-time user transactions, including withdrawals and automated processes.
- Cold wallets are used for long-term secure storage of the majority of funds.
- Hot wallets must hold only the minimum float required for operational liquidity.
- Transfers between hot and cold wallets require strict authorization and are logged.
- Supported regulated stablecoins are held segregated by asset within the custodial infrastructure and not co-mingled.

11.1.2 Multi-Signature and Multi-Party Authorization

- Multi-signature wallets or secure multi-party computation (MPC) solutions must be used for large withdrawals, cold-wallet movements, and funding of hot wallets.
- Signature thresholds must be defined based on risk tier.
- No individual may have unilateral authority to move significant funds.

11.1.3 Cryptographic Credential Protection

- Cryptographic credentials must be stored within a regulated, audited custody platform.
- No private key may be exported, stored on local devices, or shared or transmitted.
- Backup keys must be encrypted and stored separately under strict access controls.

Access to key-management systems must require MFA and role-based privileges.

11.1.4 Withdrawal Approval Procedures

A structured, tiered approach to withdrawal approvals is applied:

Tier 1 - Low-value withdrawals

- Processed automatically by system rules.
- Subject to AML, sanctions, and mixer screening.

Tier 2 - Medium-value withdrawals

- Require manual review by Finance or AML team.
- Additional transaction-velocity and behavioral checks apply.

Tier 3 - High-value withdrawals

- Require multi-signature or multi-party approval.
- Mandatory AML and EDD review.
- Potential request for source-of-funds verification.

Tier 4 - Exception withdrawals

- Suspicious transactions.
- Requests from flagged accounts.
- Blocked pending further investigation.

All withdrawals must be logged and auditable.

11.2 Transaction Controls

This section describes the information security controls that protect the AML/CFT transaction control systems. The substantive AML/CFT obligations themselves - including CDD triggers, sanctions screening procedures, mixer detection thresholds, velocity rules, and Unusual Transaction Reporting via goAML - are governed by the AML/CFT Policy. This section ensures that those controls operate on a secure, tamper-resistant, and auditable technical foundation.

11.2.1 Integrity of AML Monitoring Systems

- Transaction monitoring systems run on production-segregated infrastructure with role-based access restricted to the Compliance Officer and authorised AML personnel.
- Detection rule configuration is held in version-controlled repositories; rule changes require change-management approval and are logged.
- Monitoring system outputs (alerts, scores, flags) are written to tamper-resistant logs.
- Alert routing and escalation flows are tested as part of periodic incident response drills.

11.2.2 Security of Sanctions and Wallet-Risk Screening Integrations

- Integrations with sanctions data providers and blockchain analytics providers operate over authenticated, encrypted channels (TLS 1.2 or higher) with credentials stored in secure vaults.
- Provider API keys are rotated on a defined schedule and on any indication of compromise.
- Screening responses are recorded immutably to support post-hoc audit and dispute resolution.
- Provider availability is monitored; failure of a screening integration triggers transaction holding rather than silent bypass.

11.2.3 Protection of AML Investigation Data

- Player records under AML investigation, EDD documentation, and source-of-funds artefacts are classified as Highly Confidential under Section 5.3.4.
- Access is restricted to the Compliance Officer and authorised AML investigators on a need-to-know basis.
- Investigation case files are stored in encrypted form with access logged.
- Tipping-off controls prevent investigation indicators from being exposed in player-facing systems or communications.

11.2.4 Security of Reporting Channels

- Connectivity to the FIU goAML reporting portal operates from designated, monitored workstations under privileged access controls.
- Filer credentials are personally held by the Compliance Officer (or delegated authorised filers) and are not shared.
- All filings are recorded internally with timestamp, filer identity, and submission reference.
- Backup access arrangements are documented to maintain reporting capability during staff absences.

11.3 Funds Protection Measures

11.3.1 Segregation of Player Balances

Player funds must be separated from operational or corporate funds.

- Player balances held in custody must not be used for operating expenses, investments, or salaries.
- Systems must maintain a real-time ledger of segregated balances.
- Custody accounts must be reconciled at least daily on any day with transaction activity.

11.3.2 Tamper-Proof Audit Trails

All financial activity must be fully logged. Audit logs must include:

- Deposits.
- Withdrawals.
- Internal transfers.
- Wallet replenishments.
- Cold-to-hot wallet movements.
- Failed or blocked transactions.
- AML and sanctions screening results.

Logs must be immutable, encrypted, stored in secure environments, and accessible only by ISO, AML, and authorised finance personnel. Records of these logs that fall under LOK requirements must be held on the Curacao Tier-IV server.

11.3.3 Custody Provider Controls

Digital-asset custody is provided through a regulated infrastructure provider that offers, at a minimum:

- Multi-party computation (MPC) or hardware security module key protection.
- Transaction whitelisting.
- Role-based access management.
- Audit logging.
- Biometric or cryptographic authorisation.
- Withdrawal policy enforcement.
- Advanced fraud and risk controls.

The provider must integrate seamlessly into the AML and risk workflow and segregate supported stablecoins by asset.

11.3.4 Reconciliation and Financial Integrity

Reconciliation must ensure that all balances and transactions match across:

- Blockchain records.
- Internal systems.
- Custody-provider logs.
- Accounting records.

Discrepancies must be escalated immediately and investigated by Finance and Security teams.

11.4 Incident Response for Crypto Assets

Any abnormal wallet or transaction-related activity must trigger immediate incident protocols.

Triggers

- Unauthorised withdrawal attempts.
- Suspicious account behavior.
- Custody-platform alerts.
- AML flags indicating high-risk exposure.
- Failed multi-signature approvals.

Actions

- Freeze affected wallets or accounts.
- Escalate to the Compliance Officer.
- Notify senior management.
- Conduct forensic review using blockchain analytics.
- Document and store all evidence.
- Where the incident is reportable, file the incident report with the CGA within 24 hours.

12. Logging, Monitoring, and Alerting

Comprehensive logging and real-time monitoring of all critical systems is maintained to detect unauthorised activity, protect player funds, maintain fairness of gameplay, and ensure compliance with regulatory and AML/CFT obligations. All logs must be tamper-resistant, securely stored, and accessible only to authorised personnel.

12.1 Real-Time Monitoring Requirements

12.1.1 Login Attempts

- Successful and failed authentication attempts.
- MFA failures and resets.
- Brute-force detection.
- Geographic anomalies, including sudden logins from new regions.

- Device-fingerprint mismatches.

Suspicious login activity must generate alerts.

12.1.2 Wallet Movements

All deposit, withdrawal, and internal wallet transactions must be monitored in real time.

- Incoming deposits, screened for risk.
- Outgoing withdrawals, with multi-signature approval and AML checks.
- Hot-to-cold and cold-to-hot wallet transfers.
- Attempted unauthorised wallet access.
- Rapid or unusual transaction velocity.

Abnormal wallet behavior triggers immediate compliance review.

12.1.3 Administrative Actions

Admin-panel activity must be logged and monitored with elevated scrutiny.

- Account suspensions and unlocks.
- Manual withdrawal approvals.
- Changes to prize pool logic.
- Modifications to game settings or platform rules.
- Access to PII or confidential data.
- Changes to system configurations.

12.1.4 System Performance

- Server load.
- API response times.
- Memory and CPU usage.
- Database performance.
- Error rates and application crashes.
- Uptime tracking.

Performance anomalies may indicate security incidents.

12.1.5 Game Session Irregularities

- Abnormal win rates.
- Rapid-fire wagering patterns.
- Exploits or bot behavior.
- Collusion or multi-account activity.
- Abnormal return-to-player shifts.

Any anomaly linked to potential fraud or manipulation must be escalated.

12.2 Log Requirements and Retention

12.2.1 Mandatory Logs

Logs must be generated for:

- Login events.
- Admin actions.
- Wallet transactions.
- Game outcomes and RNG seeds or hashes, where applicable.
- Incoming and outgoing API calls.
- System errors and warnings.
- AML flags and compliance actions.
- Withdrawal processing and approvals.

12.2.2 Retention Periods

Retention periods are aligned with the GCB AML/CFT Regulations, the LOK, and recognised audit expectations:

- AML-related logs (transactions, KYC, EDD, UTR reviews and filings, sanctions screening): minimum 5 years.
- Player and gaming-transaction records are retained on the Tier-IV Curacao server for the period required by the CGA, and in any event no shorter than the AML retention obligation.
- Security incident logs: minimum 5 years.
- Standard operational logs: retained for a period appropriate to operational, audit, and investigative needs.
- Backup logs: retained for a period sufficient to support recovery validation and audit.

Retention may be extended for legal, AML, or audit requirements.

12.3 Tamper-Proof Logging

Tamper-Proof Measures

- Logs stored in immutable storage (append-only or write-once-read-many).
- Access restricted to ISO, Compliance Officer, and senior technical leads.
- Cryptographic signing or hashing of log batches.
- Offsite backups of logs.
- Log access and modification attempts logged separately.

Any evidence of tampering is classified as a critical incident and must be escalated immediately.

12.4 Blockchain Intelligence Integration

Blockchain monitoring capability must be integrated into all deposit and withdrawal processing pipelines to identify, assess, and mitigate AML/CFT risks in real time.

Monitoring must include detection of:

- Exposure to sanctions-listed entities.
- Mixer, tumbler, or privacy-enhancing services.
- Darknet or other high-risk address associations.
- Known fraud networks and scam typologies.
- Stolen or compromised funds indicators.
- Wallet-clustering behavior and transaction-history scoring.

The monitoring solution must provide:

- Automated risk scoring and classification.
- Real-time alerts and escalation triggers.
- Automated blocking or holding of high-risk transactions.
- Historical analysis of wallet and transaction behavior.

This capability is a mandatory component of AML and CFT controls and is required for risk detection, reporting, and ongoing compliance.

12.5 Automated Alerts and Threshold Monitoring

Threshold Alerts Must Trigger For

- Multiple failed login attempts.
- Sudden spikes in withdrawal requests.
- Large single-value withdrawal attempts.
- Wallet movements outside normal operational limits.
- Game integrity anomalies.
- System performance degradation.
- Unrecognised API calls.
- Patterns consistent with bonus abuse.
- Repeated AML flags from a single user.
- Multiple accounts linked by device or IP.

Alert Severity Levels

- Critical: requires immediate investigation, including wallet anomalies and admin misuse.
- High: prompt action, including game-manipulation and performance alerts.
- Medium: action on a same-business-day basis where reasonably practicable.
- Low: action during the next scheduled review.

Alerts must be logged, investigated, and documented.

12.6 Centralised Monitoring

All logs and alerts must be aggregated into a centralised SIEM solution with the following functions:

- Correlation of security events.
- Detection of multi-step attack patterns.
- Flagging of privilege escalation.

- Monitoring of insider threats.
- Behavioral baselining.
- Automated incident timeline creation.

The SIEM platform must operate continuously and generate real-time notifications.

12.7 Regular Review of Logs and Alerts

- Daily automated review of critical logs.
- Periodic review of admin actions, with frequency calibrated to operational scale and risk.
- Monthly reporting to senior management.
- Quarterly deep dive for compliance.
- Annual audit with external oversight where required.

All findings must be documented along with corrective actions.

13. Incident Response Plan

A structured Incident Response Plan (IRP) is maintained to ensure rapid detection, containment, and resolution of security events. The plan ensures protection of player data, continuity of operations, and compliance with CGA requirements.

This plan applies to all systems and environments, all staff, contractors, and vendors, and all incidents affecting security, operations, data integrity, financial systems, or player trust.

13.1 Incident Categories

13.1.1 Security Incidents

Events impacting confidentiality, integrity, or availability:

- Unauthorised system access.
- Privilege escalation.
- Malware infections.
- DDoS attacks.
- API abuse.
- Suspicious admin activity.
- Server compromise.

13.1.2 Operational Incidents

Events affecting service delivery:

- Server outages.
- Game-provider API downtime.
- System misconfigurations.
- Deployment failures.
- Payment-processing delays.

13.1.3 Data Breaches

Confirmed or suspected exposure of:

- Player PII.
- Wallet transaction data.
- Admin credentials.
- Logs containing sensitive information.

13.1.4 Fraud and Financial Incidents

Events involving:

- Abnormal win patterns.
- Bonus abuse.
- Multi-accounting.
- Suspicious wallet activity.
- Suspicious withdrawals.
- AML flags requiring escalation.
- Stolen-crypto exposure.
- Account takeover.

Fraud incidents require coordination with AML and Compliance teams.

13.2 Incident Reporting Channels

All employees and vendors must report suspected incidents immediately using one of the following channels:

- Internal incident-reporting system (ticket or form).
- Direct contact with the Incident Response Lead.
- Email to the dedicated security mailbox.
- Automated alerts from monitoring or SIEM tools.
- Escalation from AML or compliance systems.

No employee may ignore or delay reporting a potential incident.

13.3 Continuous Escalation Procedure

An escalation pipeline is maintained, based on automated alerting at all times with on-call coverage during defined hours and a documented response procedure for alerts raised outside those hours.

Tier 1 - Automated Detection or Support Escalation

- SIEM, monitoring tools, AML alerts.
- Support team flags suspicious behavior.
- Logged immediately and sent to the on-call responder.

Tier 2 - Incident Response Lead

- Reviews severity.

- Takes immediate action, including freezing accounts, blocking IPs, or disabling API keys.
- Notifies the ISO, Compliance Officer, and senior technical lead.

Tier 3 - Executive and Regulatory Escalation

Triggered for:

- Data breaches.
- Theft or fraud cases.
- Major outages.
- High-value wallet compromises.
- Regulatory exposure.

Escalation to:

- CEO or Managing Director.
- Compliance Officer.
- Legal team.
- Curacao Gaming Authority where required.

13.4 Communication Plan

Internal Communication

- Dedicated secure channel for incident coordination.
- Incident Response Lead provides updates to the ISO and senior technical lead.
- Daily updates during ongoing critical incidents.

External Communication

Only designated personnel may communicate with players, partners, vendors, the public, or authorities.

External communication must:

- Be approved by senior management.
- Avoid speculation.
- Provide clear, accurate information.
- Maintain confidentiality.

Player Notification

If player impact occurs:

- Affected users must be notified promptly.
- Steps for protection, including password resets and MFA, must be provided.
- Wording must align with regulatory expectations.

13.5 Response Timeline Expectations

The following internal response timelines apply:

- Critical: immediate response, with the Incident Response Lead engaged and containment measures initiated as soon as practicable. Investigation completed promptly thereafter, in time to support the 24-hour CGA notification under Section 13.8 where applicable.
- High: prompt response and mitigation, with investigation completed without undue delay.
- Medium: response on a same-business-day basis, with mitigation and investigation completed proportionate to severity.
- Low: response and resolution on a routine basis, addressed in scheduled review cycles.

Critical incidents include wallet compromise, data breach, admin-credential theft, fraud causing material loss, and platform-wide outages.

13.6 Containment, Eradication, and Recovery

13.6.1 Containment

- Freeze affected accounts.
- Disable compromised systems or API keys.
- Block malicious IPs or sessions.
- Isolate infected servers from the network.
- Prevent further wallet movements.
- Suspend suspicious withdrawals.
- Halt affected features, including games, deposit flow, or API endpoints.

13.6.2 Eradication

- Remove malware or malicious code.
- Revoke compromised credentials.
- Patch exploited vulnerabilities.
- Restore secure configurations.
- Update firewall and WAF rules.
- Reset admin and system passwords.
- Validate cleanup with fresh scans.

13.6.3 Recovery

- Restore systems from verified backups.
- Re-enable services gradually.
- Test stability and confirm no persistence threats remain.
- Monitor systems with heightened scrutiny.
- Document all recovery steps.
- Resume normal operations only after ISO approval.

13.7 Post-Incident Analysis and Documentation

After any major incident, a formal review must be conducted promptly, in time to inform corrective action and any required regulatory communications.

Post-Incident Review Must Include

- Root-cause analysis.
- Timeline of events.
- Systems and data affected.
- Actions taken.
- Recommendations for improvement.
- Required security enhancements.
- Staff training or process updates.

The full report must be approved by the ISO, filed for compliance records, shared with senior management, and used to update this Information Security Policy.

13.8 Regulatory Notification

Incident reports must be filed with the CGA within 24 hours of an incident where the incident involves, at a minimum:

- Gaming security breaches that have, or may have, compromised personal information of gamblers or game details, along with measures taken in response.
- Failure or loss of, or damage to, all or part of the equipment or software that has resulted, or may have resulted, in the loss of all or part of the Remote Games of Chance offered, along with measures taken in response.
- Gaming-related fraud or attempted fraud, or other forms of criminal behavior by players, along with measures taken in response.
- Any other behaviors or events that may pose a serious threat to the responsible, reliable, and verifiable organisation of the Games of Chance offered, or that may undermine public trust in the licensed Games of Chance.

Incident notification to the CGA must include:

- Nature of the incident.
- Time and date of discovery.
- Systems and players affected.
- Immediate actions taken.
- Planned remediation.
- Expected next steps.

Communication with the CGA must be timely, accurate, and fully documented.

13.9 Continuous Improvement

- Update the Incident Response Plan regularly.
- Conduct internal drills and simulations.
- Train staff annually.
- Integrate lessons learned into future improvements.
- Review new threat intelligence and apply updates.

14. Business Continuity and Disaster Recovery

A comprehensive Business Continuity and Disaster Recovery (BCDR) framework is maintained to ensure uninterrupted operation of gaming services, protection of player assets, and rapid restoration of critical systems in the event of a disruption. This framework applies to the Platform.

14.1 BCDR Objectives

The objectives of the BCDR program are to:

- Ensure critical systems and services remain available during disruptions.
- Protect player data, game integrity, and wallet security.
- Restore full operations within defined recovery objectives.
- Maintain continuity of casino-style games, raffle draws, leaderboard mechanics, and financial transactions.
- Satisfy regulatory expectations.
- Minimise operational and reputational impact.

14.2 Backup Strategy

14.2.1 Backup Frequency

- Databases (player accounts, transactions, game logs): frequent incremental backups and regular full backups, calibrated to recovery objectives.
- Wallet and custody-platform configuration and policy data: real-time replication.
- Application code repositories: continuous versioning.
- Infrastructure configurations (Infrastructure-as-Code, server settings): version-controlled with regular backup.
- SIEM, AML, and monitoring logs: backed up at intervals appropriate to AML and audit obligations.

14.2.2 Backup Encryption

- All backups must be encrypted using AES-256 or stronger.
- Encryption keys must be stored in secure key management environments.
- Backups containing PII, wallet metadata, or transaction logs must never be stored unencrypted.

14.2.3 Backup Storage Locations

Backups must be stored across:

- Primary secure storage within the Curacao Tier-IV facility.
- Secondary, geographically separated storage for redundancy.
- Offline or cold storage for disaster-class backups.

This ensures redundancy even in the event of regional outages while preserving data-residency obligations.

14.3 Restoration Procedures

In the event of system failure, data corruption, or an incident requiring rollback:

Restoration Steps

- The ISO or Technical Lead initiates the recovery protocol.
- The integrity of the backup version to be restored is validated.
- Databases, services, or configurations are restored in priority order.
- Integrity checks and system behavior validation are conducted.
- Public access is re-enabled only after security verification.
- Restoration steps are documented and filed in the BCDR log.

Validation Requirements

- No corrupted or partial backups may be restored.
- Systems must pass health checks, QA tests, and security scans before reopening.
- Financial and wallet reconciliation must be verified before re-enabling transactions.

14.4 Redundancy and Failover Architecture

14.4.1 Infrastructure Redundancy

- Load-balanced servers for application delivery.
- Multi-zone cloud deployment with at least two availability zones, configured to maintain data-residency requirements for the in-scope record set.
- Redundant database replicas.
- Failover routing managed by automated systems.
- High-availability custody-provider infrastructure.

14.4.2 Failover Trigger Conditions

Automatic failover activates when:

- A primary server or zone becomes unreachable.
- Database health checks fail.
- The platform experiences major performance degradation.
- A security incident requires isolation of a compromised environment.

14.4.3 Manual Failover

Manual override may occur for planned maintenance, emergency system isolation, or major updates affecting production infrastructure. All failover events must be logged and reviewed.

14.5 Recovery Time and Recovery Point Objectives

The following recovery time objectives (RTO) and recovery point objectives (RPO) apply:

- Wallet and crypto infrastructure: highest recovery priority, with real-time replication to minimise data loss and rapid restoration of custody operations.

- Raffle draw logic and prize pools: high recovery priority, with minimal acceptable data loss given the integrity sensitivity of pool balances.
- Game engines: high recovery priority, restored before re-opening gameplay to players.
- Authentication and player login: standard recovery priority.
- Admin panels and monitoring: standard recovery priority.
- Non-critical content (marketing, public pages): lower recovery priority, restored after core gaming and financial systems.

14.6 Continuity of Raffle and Casino Operations During Outages

14.6.1 Raffle Draw Continuity

If raffle operations are disrupted:

- All ticket entries and coin balances must be preserved in secure, replicated databases.
- Prize-pool amounts must remain unchanged and tamper-proof.
- Raffle draws must not occur until systems are fully restored and validated.
- Users must be notified of any rescheduled draw.
- Draw algorithms must log the timestamp of execution to maintain fairness.

14.6.2 Casino and Rivals Operations Continuity

If Casino or Rivals systems fail:

- All active bets and spins must be resolved fairly upon recovery.
- Incomplete sessions must be logged and reconciled automatically.
- Player coins and balances must remain consistent across recovery.
- Leaderboard positions are preserved across recovery.
- Third-party game providers must be notified.
- Failed or interrupted transactions must be revalidated upon restoration.

14.6.3 Wallet and Financial Continuity

Critical wallet operations follow special rules:

- All pending withdrawals must pause during outages.
- Deposits must remain visible but may be delayed in settlement.
- Any in-flight blockchain transactions must be reconciled upon recovery.
- Systems must prevent double-counting or double-spending.

14.7 Disaster Classes and Response Procedures

14.7.1 Minor Incident

- Single-service disruption.
- No data loss.
- Resolved with standard restore procedures.

14.7.2 Major Incident

- Database outage.
- Region failure.
- Extended downtime of game provider.
- Requires multi-team coordination.

14.7.3 Disaster Scenario

- Region-wide outage.
- Custody-provider downtime.
- Breach requiring full environment rebuild.
- RTO and RPO timelines must be strictly followed.

14.8 Staff Roles During BCDR Events

- Incident Response Lead: coordinates activation of the BCDR plan.
- Information Security Officer: ensures security compliance during restoration.
- Technical Lead: manages system recovery and failover.
- Compliance Officer: monitors financial and transaction integrity, including UTR-related obligations.
- Customer Support Lead: prepares player communication.
- Senior Management: approves public statements where needed.

14.9 Testing and Review

Testing Requirements

- Annual full BCDR simulation.
- Quarterly backup restoration tests.
- Periodic failover testing in staging, with frequency calibrated to operational scale and infrastructure changes.
- After any major architecture change.

Review Process

- Post-test reports must be documented.
- Improvements must be implemented.
- Senior management must sign off on BCDR updates.

14.10 Continuous Improvement

BCDR policies must be reviewed annually or after:

- Incidents.
- Infrastructure changes.
- Regulatory updates.
- Custody-provider changes.

- New gaming integrations.

BCDR documentation must always reflect the current operational model.

15. Data Protection and Retention

Although Curacao is not subject to the EU General Data Protection Regulation, the CGA and the GCB AML/CFT Regulations require operators to implement strong data-protection controls and minimum record-retention periods. The Company applies recognised data-protection principles aligned with international best practice, while ensuring full compliance with Curacao gaming and AML obligations. This section applies to all personal, financial, gaming, transactional, and operational data processed in connection with the Platform.

15.1 Data Protection Principles

The following principles are applied:

- Lawfulness, fairness, and transparency.
- Purpose limitation.
- Data minimization.
- Accuracy.
- Integrity and confidentiality.
- Storage limitation.
- Accountability.

All staff and vendors must adhere to these principles.

15.2 PII Minimization

Personal data collection, storage, and processing is limited to what is strictly required for:

- Account creation.
- Fraud prevention.
- AML and KYC compliance.
- Transaction and gameplay monitoring.
- Regulatory reporting.
- Customer support.

Data Minimization Rules

Personal data collection follows a tiered KYC model defined in detail in the KYC/AML Policy. The data set captured at each stage is as follows:

- Level 1 (signup, before any free ticket is issued): name, date of birth, address, and PEP and sanctions screening. This minimal data set applies to all players, including those participating in the free-to-play phase.
- Level 2 (identity document and biometric verification): triggered when (a) the player makes their first withdrawal of any amount, (b) the GCB AML/CFT threshold of NAF 4,000 in cumulative

deposits or withdrawals is reached, (c) suspicious activity is detected, or (d) the player becomes eligible for any prize on Weeekly, Rivals, or Casino.

- Bundle purchases, ticket re-entry, or other paid actions do not, on their own, trigger Level 2; the four Level 2 triggers above are exhaustive.
- Additional data, including enhanced due diligence artefacts and source-of-funds documentation, is collected only where required by the AML/CFT Program.
- Sensitive personal information that is not required for gaming, AML, or compliance purposes is not stored.
- Developers must never use production PII in staging or development environments.
- PII access follows the need-to-know principle.

This section governs the security treatment of the data captured at each KYC level. The triggers, processing flow, and onboarding sequence themselves are governed by the KYC/AML Policy and the Free-to-Play Terms.

15.3 Data Retention Schedule

15.3.1 Retention Timeframes

Retention periods are aligned with the GCB AML/CFT Regulations (minimum 5-year retention), the LOK record-keeping obligations, and recognised audit expectations:

Data Type	Minimum Retention	Notes
Transaction and blockchain logs	5 years	GCB AML/CFT Regulations
KYC, EDD, and source-of-funds records	5 years (post-account closure)	GCB AML/CFT Regulations; applies to both Level 1 and Level 2 artefacts
UTR filings, sanctions screening results, AML investigations	5 years	GCB AML/CFT Regulations
Gaming logs (bets, spins, RNG outputs, draw records)	Held on Curacao Tier-IV server; minimum 5 years	LOK record-keeping requirements
Player account information and profile data	Active period plus 5 years	Aligned with AML retention
Customer support tickets	2 years	Operational requirement
Security and access logs	Period appropriate to operational, audit, and investigative needs	Calibrated to operational and audit requirements
Financial and accounting records	7 years	Standard accounting practice

Data Type	Minimum Retention	Notes
Backups	30 to 365 days	Depending on backup tier

Retained data must be encrypted, access-controlled, and stored securely. Records subject to LOK regulations must be held on the Curacao Tier-IV server.

15.4 Secure Disposal and Data Destruction

At the end of the retention period, data must be securely disposed of or anonymised.

Requirements

- Electronic records must be securely wiped using industry-standard deletion protocols.
- Physical documents, where any exist, must be shredded or destroyed.
- Backups containing expired data must be securely overwritten or rotated out.
- Vendors must provide proof of destruction for any data processed on their systems.
- Destruction must be documented in a Data Disposal Log.

No expired or unnecessary data may remain in production systems. Destruction must not occur for records still subject to AML, gaming, or accounting retention.

15.5 Player Data Access, Export, and Correction

Although Curaçao does not impose GDPR obligations, the Company applies recognised user-rights principles to ensure transparency and trust, subject to AML and regulatory constraints.

Player Rights Provided

- Right of access: players may request a copy of personal data held by the Company.
- Right to correction: incorrect information may be updated upon request.
- Right to erasure (limited): players may request deletion of their account data unless it must be retained for AML obligations, transaction history, fraud investigations, or other regulatory requirements.
- Right to data portability: players may request an export of their account history.

Verification Requirements

Before fulfilling any request, the Company must:

- Verify account ownership.
- Ensure no AML/CFT obligation prevents deletion.
- Confirm the user is not subject to a compliance investigation.

Requests must be fulfilled within 30 days unless extended for complexity.

15.6 Player Data Export Controls

Controls

- Export requests must be logged.

- Only authorised personnel (Compliance Officer or Support Lead) may initiate exports.
- Files must be encrypted before delivery.
- Export delivery must use secure channels (encrypted email or secure download link).
- Sensitive fields must be masked where unnecessary.

No PII may be exported to third parties without legal justification and security agreements.

15.7 Secure Backup Handling

Backup Security Requirements

- All backups must be encrypted with AES-256.
- Access to backup storage must be role-based and MFA-protected.
- Backups must not be stored on personal or portable devices.
- Backup logs must record creation time, storage location, and access attempts.
- Backups must be stored in secure regions consistent with LOK data-residency requirements for in-scope records.
- Backups containing expired data must be rotated out according to retention schedules.

Backups must be tested periodically to ensure restorability (see Section 14).

15.8 Data Sharing With Third Parties

Any sharing of player or operational data must be:

- Purpose-limited.
- Restricted to essential operational partners.
- Covered by a Data Handling Agreement.
- Logged and auditable.
- Reviewed by the ISO and Compliance Officer.

Examples of permitted sharing include KYC vendors for identity verification, blockchain analytics providers for AML compliance, game aggregators for session and win/loss data, and payment processors for transaction confirmations.

Unauthorised sharing is strictly prohibited.

15.9 Confidentiality and Access Controls

- Access to PII must be limited to minimum required personnel.
- PII must not be visible to developers, external consultants, or game providers.
- Viewing or exporting PII must be logged.
- Admin access to PII requires MFA and special privileges.
- Sensitive data must never be transported unencrypted.

15.10 Regular Audits and Compliance Review

- Annual audit of data retention and destruction processes.
- Quarterly review of data classification and access logs.

- Vendor compliance audits verifying proper data handling.
- The security team must review whether systems collect unnecessary data.
- Policy updates must occur after system changes or regulatory updates.

16. Staff Security Training

All employees, contractors, and privileged users must understand their security responsibilities and possess the necessary knowledge to protect platform integrity, player data, and financial systems. Security training is mandatory at multiple stages of employment and is reinforced regularly. These requirements align with the permanent-education obligation, which requires annual training covering, among other topics, anti-bribery, crime prevention, responsible gaming, anti-money laundering, communication with players, and responsible advertising.

16.1 Mandatory Onboarding Training

Every new employee or contractor must complete security training before receiving access to systems.

Training Topics

- Overview of the Information Security Policy.
- Data protection rules, including PII handling and confidentiality.
- Access control requirements.
- Secure communication practices.
- Use of MFA, password policies, and account rules.
- Reporting suspicious activity or incidents.
- Anti-fraud overview relevant to gaming operations.
- AML red flags and escalation channels.
- Prohibited practices, including password sharing, key storage, and unauthorised exports.

Completion must be logged and verified by HR and the ISO.

16.2 Annual Refresher Training

All staff must complete annual security training to stay updated on:

- Policy changes.
- Emerging cyber threats.
- Updates to Curacao regulatory requirements.
- New internal procedures.
- Changes to AML or KYC rules.
- New gaming or wallet security risks.
- Mental wellbeing, anti-bribery, crime prevention, responsible gaming, AML, communication with players, and responsible advertising.

Refresher training is mandatory for all roles, including contractors and temporary staff.

16.3 Phishing and Social Engineering Awareness

Phishing Training Must Cover

- Identifying malicious emails or messages.
- Recognising fake admin or wallet alerts.
- Avoiding social engineering traps via email, SMS, or messaging platforms.
- Reporting suspected phishing attempts.

16.4 Secure Coding Training for Developers

Topics Include

- OWASP Top 10 vulnerabilities.
- SEI CERT coding standards.
- Secure API design.
- Safe handling of secrets and API keys.
- Secure CI/CD usage.
- Avoiding injection vulnerabilities.
- Server-side versus client-side security responsibilities.
- RNG protection considerations.
- Game fairness and integrity mechanics.
- Wallet and blockchain integration security.

Training must be completed during onboarding and refreshed annually.

16.5 Remote Work and Device Security

Device Requirements

- Company-managed devices are preferred.
- If personal devices are approved, mandatory device encryption, an updated operating system, active endpoint protection, and screen-lock are required.
- No public or shared computers may be used for administrative access.

Network Requirements

- Remote staff must use a secure private Wi-Fi connection and an enforced VPN for all administrative or system access.
- Public Wi-Fi is prohibited for admin console access, internal-system access, and handling player data.

16.6 Role-Based Training Requirements

Customer Support

- Safe account-recovery procedures.
- Identity confirmation methods.
- PII handling and masking.

- Fraud-detection basics.

Compliance and AML Teams

- Deep AML and CFT training.
- Wallet risk scoring.
- Suspicious activity handling.
- Transaction monitoring tools.
- Regulatory obligations under the LOK and the GCB AML/CFT Regulations.

Admin Users

- Privileged-access best practices.
- Logging and audit requirements.
- Safe modification of backend systems.

16.7 Policy Acknowledgement

All employees must formally acknowledge:

- Understanding the Information Security Policy.
- Compliance with internal procedures.
- Agreement to confidentiality obligations.
- Awareness of consequences for violations.

HR must maintain documentation of each acknowledgement.

16.8 Tracking and Reporting

- All training completion records must be stored securely.
- The ISO must review training participation periodically.
- Non-compliant staff must be flagged and followed up with.
- Training materials must be updated annually.

16.9 Consequences for Non-Compliance

Failure to comply with security-training requirements may result in:

- Removal of system access.
- Mandatory retraining.
- Disciplinary action, up to and including termination, depending on severity.

17. Physical Security

The Company's operations are predominantly cloud-hosted and rely on infrastructure providers for physical security of the underlying environment. Where the Company maintains physical office space, including its registered office in Curaçao, access is restricted to authorised personnel. Workforce devices (laptops, mobile devices, and hardware authentication keys) are inventoried in the Information Asset

Register, encrypted at rest using full-disk encryption, and remotely lockable in case of loss or theft. Devices used for privileged access to financial systems, including transaction signing, are subject to enhanced controls. Any printed records containing sensitive data are stored in locked cabinets and disposed of adequately.

Background checks are conducted, proportionate to role risk, for new hires and contractors in critical or sensitive roles such as those with production, wallet, finance, or compliance responsibilities. All personnel sign confidentiality agreements at onboarding. On termination or role change, company-issued devices and hardware tokens are reclaimed and recovery is recorded in the offboarding log.

18. Change and Configuration Management

Strict change and configuration management procedures are maintained to protect system stability, prevent unauthorised modifications, and maintain auditability. These controls apply to infrastructure, application code, game engines, wallet systems, and administrative configurations, and feed into the operations-manual amendment reports (filed twice yearly, no later than 15 June and 15 January).

18.1 Approval Process for Updates

All changes, including code, infrastructure, and configuration, must follow a documented approval workflow.

Requirements

- A Change Request must be submitted describing purpose, impact, and testing plan.
- Approval is required from the Technical Lead, the ISO for sensitive changes, and the Compliance Officer for changes related to financial or AML systems.
- High-risk changes must undergo peer review and formal management approval.

18.2 Version Control

Controls

- Mandatory use of secure source-control repositories.
- Branching strategies for development, staging, and production.
- Every change must be traceable to a user and ticket.
- Sensitive files must not be stored in version control, including API keys and passwords.
- Commit history must be retained indefinitely.

18.3 Production Deployment Rules

Requirements

- Production deployments must pass automated tests, code reviews, and security scans (SAST and DAST), and must be approved by the Technical Lead.
- No developer may deploy directly to production without authorisation.
- Deployments must be logged, monitored, and performed using CI/CD pipelines with MFA.

- The production environment must not allow ad-hoc manual code changes.

18.4 Emergency Change Procedures

In emergencies, including critical bugs, outages, or security threats:

- An Emergency Change Request may be submitted.
- The ISO and senior technical lead must approve expedited deployment.
- Monitoring must verify system stability post-deployment.
- Full documentation must be completed retroactively within 24 hours.
- Emergency changes are subject to post-implementation review.

18.5 Configuration Management

- Baseline configurations must be documented and stored in secure repositories.
- Unauthorised configuration changes are prohibited.
- Configuration changes must be tracked through version control.
- Sensitive components, including firewalls, WAFs, servers, and wallet integrations, must follow a strict approval path.
- Drift-detection tools should monitor for unauthorised changes.

18.6 Rollback Strategy

Rollback Requirements

- Every deployment must have a defined rollback plan, a previous stable version ready, and automated or manual rollback capability.
- Rollbacks must be executed if health checks fail, must be logged, and must trigger root-cause analysis.

Systems must return to a stable state with minimal downtime.

18.7 Operations Manual and Amendment Reports

The Company maintains an operations manual covering, at a minimum:

- A description of the games offered, payment options, bet amounts, payouts, software, and outcome-determining elements.
- A description of periodic test methods used for quality monitoring.
- The way of storing players' personal data and other details.
- A description of visual elements shown to players.
- Technical measures to prevent excluded persons from playing.
- A diagram of technical infrastructure and disaster recovery options.
- A description of how responsible gaming principles are implemented.
- The most recent text of the general terms and conditions.
- A description of how disputes with players are settled.
- Identification of the digital records held on the Curacao Tier-IV server.

Changes to the operations manual must be filed with the CGA in amendment reports submitted twice a year, no later than 15 June and 15 January, accompanied by a new version of the operations manual.

19. Policy Governance and Review

This Information Security Policy is maintained as a living document, reviewed regularly, and approved by senior leadership to ensure ongoing compliance with operational and regulatory requirements.

19.1 Annual Review

- This policy must be reviewed at least once per year.

The review must include:

- Updating sections to reflect new threats.
- Including new regulatory changes, including any amendments to the LOK or GCB AML/CFT Regulations.
- Updating vendor or technology changes.

Policy revisions must be documented with version history.

19.2 Review After Major Incidents

In addition to annual review, immediate review is required after:

- Security breaches.
- Major outages.
- Wallet or transaction anomalies.
- Fraud events.
- Audit findings.
- Infrastructure migrations.

Review must analyze whether existing controls were adequate and update them accordingly.

19.3 Policy Approval by Senior Management

This policy must be approved by:

- The CEO or Managing Director.
- The senior technical lead (CTO or Technical Director).
- The Information Security Officer.
- The Compliance Officer (for AML-relevant updates).

Approval must be documented and recorded. Only authorised executives may approve changes or exceptions.

19.4 Documentation Control and Versioning

All versions of this policy must be:

- Version-controlled.
- Time-stamped.
- Stored securely.
- Archived for a minimum of 5 years.
- Distributed only through secure internal channels.

Change logs must include:

- Author.
- Approver.
- Summary of changes.
- Date of revision.

19.5 Accessibility

- The latest approved version must be accessible to all staff.
- Sensitive appendices, including wallet procedures, may have restricted access.
- All employees must be notified of major changes.