

Operational Manual

Curaçao Licensing — National Ordinance (LOK) Article 5.9

FarUp Entertainment N.V.

HOLDER OF THE CURAÇAO GAMING LICENCE

DOCUMENT CONTROL

Document title	Operational Manual
Version	1.0
Date	22 June 2026
Owner	Operations, Technology, Compliance & Management functions
Classification	Confidential
Regulatory basis	Curaçao National Ordinance (LOK) Article 5.9

This Manual is an operational document maintained by the functions that run the licensed business. It is reviewed at least bi-annually and on any material change to the business, platform or operating model.

Contents

1 Purpose and Scope	3
2 Description of the Gaming Operation (LOK Art. 5.9(a))	4
3 Testing and Quality Assurance (LOK Art. 5.9(b))	6
4 Player Data Management (LOK Art. 5.9(c))	7
5 Website and Player Interface (LOK Art. 5.9(d))	9
6 Excluded and Restricted Persons Controls (LOK Art. 5.9(e))	10
7 Technical Infrastructure (LOK Art. 5.9(f))	11
8 Business Continuity and Contingency Arrangements	12
9 Responsible Gaming (LOK Art. 5.9(g))	14
10 Terms and Conditions (LOK Art. 5.9(h))	15
11 Complaints and Dispute Resolution (LOK Art. 5.9(i))	15
12 Record Keeping and Retention	16
13 Critical Information and Transaction Records (LOK Art. 5.9(j))	17
14 Data Centre and Hosting Arrangements (LOK Art. 5.9(j))	18

1 Purpose and Scope

This Operational Manual describes how the licensed gaming operation of FarUp Entertainment N.V. (the “Company”) is structured and carried out in practice. It is prepared in accordance with Article 5.9 of the Curaçao National Ordinance (LOK) and is intended to give the Curaçao Gaming Authority (CGA) a clear, practical understanding of the Company’s gaming products, operational processes, technology environment, outsourcing arrangements and internal controls.

The manual is an operational document. It is owned and maintained by the operational, technical, customer support, finance, responsible gaming and management functions that run the licensed business, with the Compliance function assisting on regulatory alignment and completeness. It is reviewed at least bi-annually and/or whenever a material change to the business, platform or operating model occurs.

1.1 The licensed operation

FarUp Entertainment N.V. holds the Curaçao gaming licence and operates online gaming brands under that licence. The Company forms part of a wider group in which Funnz Ltd (Malta) acts as the group’s managed-services and technology company, employing the development team and providing the platform, technical, operational and marketing services consumed by the licensed operating entities.

The Company offers two principal gaming verticals: an online casino (comprising video slots, live casino, table and instant win games) and a sportsbook. Its principal brands include Shotz, CasinoFriday and BetFriday, which share a common multi-brand technology architecture.

1.2 Internally managed and outsourced activities

The Company retains ownership and control of its customer-facing systems, data and commercial and operational business logic. The proprietary front-end and middleware layer — including lobby presentation, user experience, session handling, API orchestration and the customer onboarding and cashier flows — is developed and operated within the group by Funnz Ltd.

A number of supporting functions are delivered by third-party service providers under commercial agreements, with the Company retaining oversight and control of the outsourced services. The principal outsourced functions are:

- Player Account Management (PAM): Pragmatic Solutions provides the core account, wallet and transaction-processing platform, deployed in the Company's own hosting environment.
- Sportsbook: Altenar provides the sportsbook platform and trading.
- Game content: casino content is supplied by multiple studios directly and through the Relax Gaming, Hub88, Alea and Games Global aggregation hubs.
- Payments: payment orchestration and processing are provided through PIQ/Devcode
- Marketing and CRM: Optimove (with SendGrid for email and a third-party SMS provider) and Cellxpert for affiliate management.
- Infrastructure and Devops: Amazon Web Services (AWS) for hosting and Cloudflare for CDN, web application firewall and DDoS protection, supported by outsourced DevOps/Infrastructure resources via Clamtech.

For each outsourced function, the Company maintains contractual arrangements, defined provider responsibilities and operational oversight so that it retains adequate control over the outsourced activity, as described in the relevant sections below.

2 Description of the Gaming Operation (LOK Art. 5.9(a))

This section describes how the licensed operation is structured and operates on a practical level, covering the gaming products offered, the platform on which they run, the payment and settlement processes, the way game outcomes are determined, and the journey a player takes through the operation.

2.1 Gaming products and game categories

The Company offers an online casino and sportsbook. The casino comprises video slots (which make up the majority of the catalogue), live casino with human-dealer tables, and instant win or "crash"-style games as well as regular table games such as blackjack. The sportsbook offers pre-match and in-play betting across a range of sports and markets. Content is organised in the player lobby by category and provider, with curation, promotion and configuration controlled by the Company's proprietary front-end and CMS.

2.2 Software and game providers

Casino content is sourced from a broad set of studios under commercial agreements held directly between the Company (or group) and each provider or aggregator. Direct studio

integrations include Pragmatic Play, Play'n GO, Playson, Push Gaming, Quickspin, Yggdrasil, Thunderkick, Betsoft, Booming Games, Light & Wonder and Elk Studios. Further content is delivered through the Relax Gaming, Hub88, Alea and Games Global aggregation hubs, which carry studios such as Hacksaw Gaming, Nolimit City, Big Time Gaming, Red Tiger, NetEnt, Evolution, Ezugi and PG Soft, among others. The sportsbook is provided by Altenar.

Full Provider List:

Provider	Content / purpose	Integration type	Status
Casino — direct studio integrations			
Pragmatic Play	Slots & casino games	Direct	Live
Play'n GO	Slots & casino games	Direct	Live
Playson	Slots & casino games	Direct	Live
Push Gaming	Slots & casino games	Direct	Live
Quickspin	Slots & casino games	Direct	Live
Yggdrasil	Slots & casino games	Direct	Live
Thunderkick	Slots & casino games	Direct	Live
Betsoft	Slots & casino games	Direct	Live
Booming Games	Slots & casino games	Direct	Live
Casino — aggregation hubs			
Relax Gaming	Aggregator platform / content hub	Direct	Live
Hub88	Aggregator platform / content hub	Direct	Live
Alea	Aggregator platform / content hub	Direct	Live
Games Global	Game aggregation &	Direct	Live

	content hub		
Light & Wonder	Aggregator platform / content hub	Direct	Live
Casino content via Relax Gaming			
4ThePlayer	Slots & casino games	Aggregator (Relax)	Live
Big Time Gaming	Slots	Aggregator (Relax / Hub88)	Live
Fantasma Games	Slots	Aggregator (Relax)	Live
G Games	Slots & casino games	Aggregator (Relax)	Live
Hacksaw Gaming	Slots	Aggregator (Relax)	Live
Kalamba Games	Slots	Aggregator (Relax)	Live
MaxWin Gaming	Slots	Aggregator (Relax)	Live
Nolimit City	Slots	Aggregator (Relax / Hub88)	Live
Print Studios	Slots	Aggregator (Relax)	Live
Peter & Sons	Slots	Aggregator (Relax)	Live
Skywind	Slots	Aggregator (Relax)	Live
Slotmill	Slots	Aggregator (Relax)	Live
Stakelogic	Slots, Live casino & casino game	Aggregator (Relax)	Live
Swintt	Slots	Aggregator (Relax)	Live
RubyPlay	Slots	Aggregator (Relax)	Live
Revolver Gaming	Slots	Aggregator (Relax)	Live
Games Inc	Slots	Aggregator (Relax)	Live

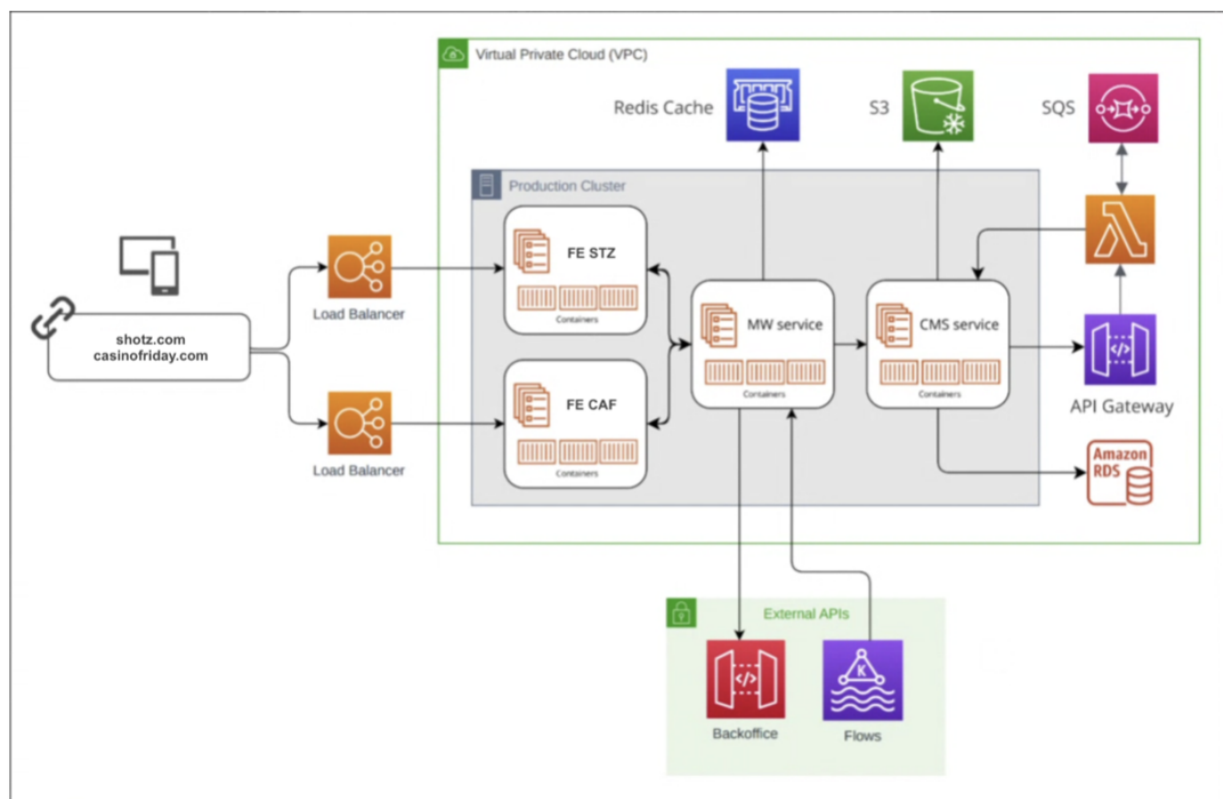
Ela Games	Slots	Aggregator (Relax)	Live
Blaze Gaming	Slots & casino game	Aggregator (Relax)	Live
Playnetic	Slots	Aggregator (Relax)	Live
Casino content via Hub88			
Evolution Gaming	Live casino	Aggregator (Hub88)	Live
Ezugi	Live casino	Aggregator (Hub88)	Live
Gaming Corps	Slots	Aggregator (Hub88)	Live
AvatarUX	Slots	Aggregator (Hub88)	Live
Spribe	Instant games	Aggregator (Hub88)	Live
JustSlots	Slots	Aggregator (Hub88)	Live
ShadyLady	Slots	Aggregator (Hub88)	Live
Red Tiger Gaming	Slots	Aggregator (Hub88)	Live
NetEnt	Slots	Aggregator (Hub88 / Games Global)	Live
Casino content via Alea			
Raw iGaming	Slots	Aggregator (Alea)	Live
Octoplay	Slots	Aggregator (Alea)	Live
PG Soft	Slots	Aggregator (Alea)	Live
Casino content via Light & Wonder			
Elk Studios	Slots	Aggregator (Light & Wonder)	Live
Sportsbook			
Altenar	Sportsbook platform & trading	Direct	Live

2.3 Platform structure

The operation runs on a modular iGaming technology stack with two clearly separated layers. Core account, wallet and transaction functionality is provided by a third-party licensed PAM platform (currently Pragmatic Solutions), deployed within the Company's own AWS hosting environment. The entire customer-facing layer — front-end websites and middleware/business logic — is proprietary, developed and owned within the group, and is intentionally PAM-agnostic.

This decoupled design allows the Company to maintain ownership and control of all customer-facing systems, data flows and operational logic while relying on the PAM provider for core account management, wallet and transaction processing and associated regulatory functionality.

High-level architecture diagram:



2.4 Payment methods

Deposits and withdrawals are supported through a payment orchestration layer (PIQ/Devcode) and connected payment service providers. The Company controls the cashier interface and the deposit and withdrawal flows through its proprietary middleware and front-end. All deposit and withdrawal transactions are processed through a direct integration into the PAM.

We offer a range of payment methods to the end user which vary depending on the jurisdiction, such as Card (Visa and Mastercard), Revolut, bank transfers, Apple & Google Pay and Interac (Canada only).

2.5 Bet and payout processes

Casino wagers are placed through the proprietary front-end, launched into the relevant game provider's environment, and recorded against the player's wallet in the PAM. Sportsbook bets are placed within the Altenar-provided interface and settled by Altenar's trading systems, with the resulting transactions (bets, settlements and balance movements) processed through the direct PAM integration. All stakes, winnings and balance changes are reflected in the player's PAM-held wallet, ensuring a single, authoritative record of financial activity. For winning Casino wagers, the winnings are credited to the player balance instantly at the end of the completed spin/game round. For winning Sportsbook wagers, the winnings are credited after the event has finished and/or the outcome has been decided and settled by the Altenar trading team.

2.6 Outcome determination mechanisms

Slot, table and instant win game outcomes are determined by random number generators operated within each game provider's certified environment; the Company does not generate any outcomes itself. Live casino outcomes are determined by the physical actions of human dealers, captured and streamed by the live-studio provider and recorded digitally for a complete footprint of every event which occurred. Sportsbook outcomes are determined by real-world sporting events and settled by the sportsbook provider's trading operation. Game and RNG fairness is evidenced by the certification held by the respective providers.

2.7 Player journey

A player's lifecycle through the operation begins on the relevant brand website, where the player creates an account through the registration flow described in Section 5.1. During registration, the player provides the personal and account information required by the interface, including name, email address, mobile telephone number, date of birth, residential address and password. The player must confirm that they are of legal age to participate in online gaming in their relevant

jurisdiction, review and accept the applicable Terms and Conditions and Privacy Policy, and select their marketing and communication preferences.

During and following registration, the platform applies the relevant account-opening and eligibility controls. These include validation of mandatory registration fields, duplicate-account checks, jurisdictional checks, exclusion or self-exclusion checks where applicable, and other account-status or risk indicators supported by the platform.

Once the account has been created, the player can access the logged-in account area, browse the casino and sportsbook lobbies, and fund their account through the cashier. Deposits are processed through the payment layer and recorded against the player's PAM-held wallet. The player may also be presented with available promotional offers during the deposit journey and can choose whether to accept an offer or proceed without a bonus.

The player can then select and launch casino games through the casino lobby or place sports bets through the sportsbook. Casino wagers, sports bets, settlements, winnings and balance movements are recorded against the player's PAM-held wallet so that the PAM remains the authoritative record of player funds and transaction activity.

Throughout the lifecycle, the player can manage their account through self-service tools, including account settings, password management, payment and transaction history, responsible-gaming controls, communication preferences and customer-support or complaint channels. Withdrawals are requested through the cashier and are processed through the payment layer and PAM, subject to account status, wallet balance, payment-method eligibility, KYC, AML, fraud, responsible-gaming and bonus-related controls where applicable. Each stage of the player journey is supported by the operational, technical and compliance controls described in the sections that follow.

3 Testing and Quality Assurance (LOK Art. 5.9(b))

This section explains how the quality and integrity of the gaming operation is monitored, including how games are certified, how the platform and releases are tested, how defects are managed, and how testing is reviewed over time.

3.1 Game certification

Games and their random number generators are certified within the environment of the relevant game provider, and the corresponding certificates are obtained from the providers (or their accredited test laboratories) and retained by the Company as evidence of fairness and integrity.

Certificates are reviewed when new content providers are on-boarded and/or when new casino games are launched on site. RNG certificates are held by the game providers.

3.2 Testing arrangements and security testing

Testing is applied proportionately to the Company's scale and risk exposure across the platform and the game catalogue. The Company conducts at least annual external vulnerability scans of its internet-facing infrastructure using a PCI-approved Approved Scanning Vendor (VikingCloud); the most recent scan was completed in December 2025. Code review is embedded within the development lifecycle. Findings are reviewed, prioritised and remediated in line with risk and operational priority.

3.3 Quality assurance procedures

Quality assurance is supported by secure coding standards and peer code review, with releases reviewed and signed off by the engineering lead. Information-security requirements are embedded into the software development lifecycle. The proprietary front-end and middleware are tested against functional and non-functional requirements before changes are promoted to production.

3.4 Release and deployment testing

Platform changes are deployed on a regular, coordinated cadence. Releases involving the PAM are scheduled with the PAM provider, and CI/CD pipelines, deployment tooling and operational scripts are owned and centrally managed within the group with role-based access.

PAM and Sportsbook development releases are fully QA tested on a staging environment by both 3rd party provider QA teams and the company's in-house development team before releasing to production. Post the production release, QA is carried out by internal teams and stakeholders to validate the changes have been made successfully.

3.5 Defect management

Defects and production incidents are managed through a structured ticketing process with the PAM provider's service desk, using priority levels P1 (Critical) through P5 (Very Low). Each Production Incident ticket records information such as the affected brand, the functionality affected, any regulation(s) impacted, the customer and revenue impact, the number of users affected, reproduction steps and the expected versus actual result, and shares the relevant stakeholders so that they are notified of each update. Real-time support is also available

through the provider's technical support channel. Front-end and middleware defects are logged, prioritised, fixed and verified by the engineering team.

Anyone within the company can raise a production incident via the ticketing process, the most frequent being our Customer Support agents who work 24/7 and speak directly to our customers. If a critical issue (P1 incident) is reported, we have 24/7 on call support to provide immediate assistance and incident management until the incident is resolved.

3.6 Periodic reviews

Testing activity is reviewed on a recurring basis. Vulnerability scan results, release outcomes and defect trends are monitored, and findings are tracked to closure. The Company's information-security and testing arrangements are reviewed periodically by management and updated as the business evolves.

4 Player Data Management (LOK Art. 5.9(c))

This section explains how player information is collected, stored, accessed, retained and protected. It is aligned with the Company's Information Security Policy and applicable privacy requirements. The Company acts as data controller for player and employee personal data, and third-party providers that process personal data do so as processors under contractual data-processing arrangements.

4.1 Categories of player data

The Company maintains the categories of player information necessary to operate the licensed business and meet its regulatory obligations, including:

- Identity and registration data (name, contact details, date of birth, verification documents);
- Financial and payment data (deposits, withdrawals, payment instruments and transaction history);
- Gameplay and account data (wagering activity, game history, balances and account status);
- Behavioural and marketing data (engagement and lifecycle signals used by the CRM platform).

4.2 Storage arrangements

All player and transactional data is stored within an Amazon Web Services (AWS) EU instance. Core databases and backend/transactional data reside in a logically isolated, access-restricted backend environment (comprising self-managed MySQL on EC2 and AWS RDS), which is separated from the front-end/middleware environment. Production, staging and development environments are logically separated.

4.3 Retention periods

Player data is retained for the periods required by applicable gaming and data-protection obligations, governed by the Company's data retention schedule. Each category of player data is assigned a retention period, after which the data is deleted or anonymised in accordance with Section 4.6.

4.4 Access controls

Admin user access to player data is granted on a least-privilege basis aligned to user role and operational responsibility. Privileged access is restricted only to relevant personnel and access rights are periodically reviewed by system owners and department heads. Access to production systems is restricted and logged and Multi-factor authentication is enforced where technically supported, including for our PAM and Sportsbook Back offices, AWS and critical third-party systems. Admin user login Credentials are held in secure password maintenance tools.

Our IT team manages the process for onboarding/offboarding new joiners and leavers to assign and remove admin access, and Heads of department are responsible for requesting and approving changes to admin permissions for example after a change of role and responsibility.

4.5 Backup procedures

Core database backups are managed by the PAM provider in accordance with its operational procedure and AWS Backup configuration. Automated backups are scheduled at least three times per day (approximately every eight hours) to meet recovery-point objectives, with backup vaults, retention policies and access permissions configured within the managed environment. The Company validates application functionality following any restoration event.

4.6 Deletion procedures

Player data is deleted or anonymised once the applicable retention period expires, in accordance with secure deletion practices. Company-issued devices that may hold operational data are managed under a Mobile Device Management solution and can be remotely restricted or wiped in the event of loss or compromise.

5 Website and Player Interface (LOK Art. 5.9(d))

This section describes the visual and operational elements presented to players through the Company's websites, including registration, account access, payments, responsible-gaming tools, complaint channels and game access.

5.1 Registration

Player registration and onboarding are presented through the proprietary front-end and are integrated into the Company's middleware, the PAM and connected verification services. The registration flow is initiated from the relevant brand website and is designed to capture the information required to create a player account, verify eligibility, establish communication preferences and support the required audit trail before the account is used for real-money play.

The player opens a "Create account" dialogue from the brand website and is guided through a structured registration flow. The interface is designed to allow registration to be completed quickly and presents the player with a clear progression through the required account-opening steps. Players who already hold an account are able to switch from the registration path to the log-in path directly from the registration dialogue.

The first stage of registration captures the core account credentials and identity details required to create the account, including the player's first name, last name, email address and password. Before the player can proceed, the interface requires explicit acceptance of the applicable Terms and Conditions and Privacy Policy, an explicit confirmation that the player is at least 18 years of age or otherwise of legal age for online gaming in their relevant jurisdiction, and completion of an anti-bot or form-validation check. The registration endpoint is protected by automated-abuse controls, including a Cloudflare "verify you are human" check where presented by the interface.

Marketing and communication consent is captured separately from mandatory account-opening confirmations. Promotional and communication preferences are not bundled into the acceptance of the Terms and Conditions or Privacy Policy. The player is presented with separate opt-in choices for marketing communications and for notifications or updates by available channels such as SMS and email. These preferences are recorded against the player's account and can be changed later through the account-management area.

The second stage of registration captures the additional personal information required for regulatory, account-management and verification purposes. This includes the player's mobile telephone number with international dialling-code selector, date of birth, residential street address, city, postcode and country of residence. The address field may be supported by address-lookup functionality, such as Google Places, to improve accuracy and reduce manual input errors.

The front-end validates required fields, format requirements and mandatory declarations before the registration request is submitted. The middleware then performs the relevant account-creation checks and passes the required data to the PAM and connected verification services. These checks include duplicate-account checks, jurisdiction and eligibility controls, age and identity-verification checks, and screening against applicable exclusion or risk indicators. Where the required checks cannot be completed, or where a check produces a restriction, the account is not permitted to proceed to normal real-money use until the issue is resolved in accordance with the Company's onboarding and KYC procedures.

Once the account has been created, the player is taken into the logged-in account area and can access the lobby, cashier, responsible-gaming tools and account-management features, subject to the account status and any applicable verification, eligibility or regulatory restrictions. Registration events, declarations, consents, account status changes and verification outcomes are recorded in the PAM and related operational systems to provide an audit trail of the onboarding journey

5.2 Account access

Registered players access their accounts through the login functionality on the relevant brand website. The login flow is provided by the Company's proprietary front-end and middleware and authenticates the player against the account records held in the PAM. Returning players can access the login path directly from the registration dialogue or from the standard login option on the website.

Players log in using their registered email address and password. A player may access the website in a logged-out state for browsing where permitted, but deposits, withdrawals, real-money gameplay, account-management functions and responsible-gaming settings

require the player to be logged in. Relevant account-status checks are performed before restricted account actions are allowed.

The account-access flow supports standard account-security controls, including password-based authentication, form validation, session handling and automated-abuse protection. The registration and login endpoints are protected by the Cloudflare anti-bot controls referenced in Section 5.1. Players can update their password at any time through the account menu using the “Password — Update” option. Where a player cannot access their account, password-reset and support-assisted recovery routes are made available through the website or customer-support channels.

Account access is restricted where the account is closed, suspended, self-excluded, subject to responsible-gaming restrictions, under review, or otherwise blocked for compliance, security or operational reasons. Player sessions and account access are managed through the front-end and middleware layer, with relevant status checks made against the PAM before account actions are allowed.

Player-facing account access is separate from the administrative and infrastructure access used to operate the platform. Administrative access to player records, back-office systems and infrastructure is controlled through the role-based access-control, least-privilege and privileged-access arrangements described in Sections 4 and 7, including multi-factor authentication where technically supported.

5.3 Deposits and withdrawals

The cashier is presented to logged-in players through the brand website and is controlled by the Company through its proprietary front-end and middleware. The cashier displays the player's current balance, the balance available for withdrawal where applicable, and the deposit and withdrawal methods available to that player. Available methods may vary according to brand configuration, jurisdiction, currency, payment-provider availability, account status and any applicable verification, responsible-gaming or compliance restrictions.

Deposit and withdrawal flows are orchestrated through the Company's proprietary middleware and front-end and processed through the payment orchestration layer, PIQ/Devcode, and connected payment service providers. Every deposit and withdrawal is recorded against the

player's PAM-held wallet so that the PAM remains the single authoritative record of player funds and financial activity.

For deposits, the player selects an available payment method, enters the required amount and payment details, and confirms the transaction. Deposit methods presented to players may include payment cards such as Visa and Mastercard, Revolut as a direct or instant payment method, Apple Pay and Google Pay, depending on availability and eligibility. Deposit limits and other responsible-gaming controls are checked before the transaction is accepted. Successful deposits are processed through the payment layer, recorded against the player's PAM-held wallet and reflected in the player's balance for gameplay.

During the deposit journey, the cashier may also present available promotional offers. For example, the player may be offered a casino welcome bonus, such as 100% up to 500 plus 200 free spins. Where an offer is available, the player can choose to opt in by enabling the corresponding bonus toggle, or can proceed with the deposit without taking a bonus. Any selected bonus is applied in accordance with the applicable bonus terms and any wagering conditions.

For withdrawals, the player accesses the withdrawal section of the cashier or account menu, where the available withdrawal balance is displayed. The player selects an available withdrawal method, enters the withdrawal amount and submits the request. Withdrawal availability is subject to the player's account status, wallet balance, payment-method eligibility, customer due diligence and source-of-funds requirements where applicable, fraud and risk checks, responsible-gaming restrictions, and any open bonus or wagering conditions.

Withdrawal requests are processed through the payment layer and PAM and are subject to the Company's customer due diligence and anti-fraud controls, including identity verification and, where required, the verification of additional information such as identity documents, source-of-funds or source-of-wealth evidence and other due-diligence checks, before any payout is released. The player-facing cashier provides transaction feedback to the player, including confirmation, failure or pending statuses where applicable.

Deposit and withdrawal events, status changes and related payment records are retained in the PAM and reporting tools. This enables operational reconciliation, customer-support review, AML and fraud monitoring, complaint investigation, and regulatory reporting where required. Players can also retrieve their own transaction history directly through the cashier or account area, giving them a complete player-facing payments history.

5.4 Responsible-gaming tools

Players can access responsible-gaming controls directly from the account interface, including through the dedicated “Play safe” tools area, and from other player-interface locations where appropriate. These tools are presented as self-service controls and are supported by platform-level enforcement in the PAM, middleware and related operational processes.

The player interface provides access to the responsible-gaming controls described in Section 9, including deposit limits, loss limits, time outs and self-exclusion. The interface explains the effect of each control before the player confirms the request, including how the control will affect deposits, gameplay, account access or future changes to the setting.

Responsible-gaming settings are applied in accordance with the Company’s Responsible Gaming Policy. Reductions in limits or more restrictive settings are applied promptly, while increases or less restrictive changes are subject to the applicable cooling-off and approval rules. Once a control has been confirmed, the restriction is reflected in the PAM and relevant operational systems so that the player cannot continue activity that is inconsistent with the selected control.

Where a player applies self-exclusion or another restrictive responsible-gaming control, the account is restricted in line with the chosen control and the procedures described in Section 9. This includes preventing further play, deposit activity or account activity where required by the control, and applying marketing suppression and reactivation controls in accordance with the Company’s responsible-gaming procedures.

The player-facing responsible-gaming tools, the way those tools take effect, and the monitoring, intervention, escalation and record keeping processes that support them are described in detail in Section 9.

5.5 Complaint submission channels

Players can contact the Company and raise complaints through the support channels presented within the account interface, including an in-product live chat (“Live Chat — chat with us”) and the Company’s other published customer-support contact methods. The

end-to-end process for logging, investigating, escalating and resolving complaints, and the associated record-keeping and oversight, is described in Section 11.

5.6 Game selection, access and account management

Games are launched through the proprietary front-end and middleware layer, with the Company retaining full control over lobby presentation, search, filtering, configuration and the overall player experience. The casino lobby organises content into categories (including casino and live casino) and provides a search function that lets players find games by title, feature or provider. The sportsbook ("Odds") presents a sports navigation bar (covering football, tennis, ice hockey, e-sports, basketball, baseball, golf and other sports), top-league shortcuts, live and upcoming events with prices, and a bet slip that supports single, combination and system bets, showing stake, potential winnings and total return before a bet is placed. Promotions, rewards and campaign areas are surfaced alongside the casino and sportsbook lobbies.

When a game is launched it runs within the Company's client, with the account and navigation shell (balance, deposit access and lobby navigation) presented around it; casino games are supplied by the integrated providers (for example Pragmatic Play) and launched through the proprietary front-end as described in Section 2.

6 Excluded and Restricted Persons Controls (LOK Art. 5.9(e))

This section explains how the operation prevents participation by prohibited or restricted individuals, including minors, self-excluded players and players in restricted jurisdictions.

6.1 Age and identity verification

Before a player is permitted to play, the Company applies age and identity controls at the point of registration. During registration, players are required to confirm they meet the legal gambling age (18 or older, or higher where required by their jurisdiction). The system enforces this in two ways: it validates the date of birth entered by the player against the applicable minimum age, and it requires the player to actively acknowledge their age by ticking a dedicated "I am over 18" checkbox before registration can be completed.

A further control applies at the point of first deposit. Before a first deposit is accepted, the player must confirm details of their payment method. As payment methods are linked to the player's own bank, card or account, this provides an additional point at which inconsistent or ineligible details may surface.

In addition, verification documentation will be requested from the player where:

- concerns remain that the player may be a minor even after the above checks;
- the player makes a first withdrawal; or
- a threshold specified in the Company's KYC and AML Policy is breached.

The documentation requested depends on the nature of the trigger and the applicable requirements. As a minimum, a valid government-issued identity document and proof of address are requested on a player's first withdrawal, and further documentation, such as payment-method or source-of-funds evidence, may be required depending on the circumstances.

Beyond these age controls, players are subject to identity and player-risk verification in accordance with the Company's AML, KYC and player-risk procedures. Verification is triggered on a risk-based basis, including where AML thresholds are met, where withdrawal amounts or cumulative activity require verification, where account information requires confirmation, or where fraud, compliance or responsible-gaming indicators require further review.

Where verification is required, the player may be asked to provide identity, age, address, payment-method or source-of-funds documentation, depending on the nature of the trigger and the applicable requirements. Accounts that do not complete required verification, or where verification identifies a restriction, may be limited, suspended from withdrawal processing, or otherwise restricted until the matter is resolved in accordance with the Company's KYC and AML procedures.

These controls are described more fully in the Company's Responsible Gambling Policy and in its general KYC and AML Policy, both of which have been submitted to the CGA.

6.2 Self-exclusion and exclusion lists

Players may self-exclude through the responsible-gaming tools available in the player account area, including the dedicated Responsible Gaming section. The interface allows the player to select the available self-exclusion option and explains the effect of the exclusion before the request is confirmed.

Once a self-exclusion is applied, it is enforced at account level through the PAM and related operational systems. The account is restricted for the duration of the exclusion period to prevent further real-money play, deposits and other activity that is inconsistent with the exclusion. Direct marketing to the player is also suppressed for the exclusion period in accordance with the Company's responsible-gaming procedures.

Self-exclusion status is recorded against the player account and is visible to authorised operational and customer-support users where required for account handling. Attempts to reactivate, reopen or otherwise use an excluded account are subject to the applicable

reactivation rules and checks. The Company also applies duplicate-account and account-linking controls to help identify attempts to circumvent an active self-exclusion by opening or using another account.

6.3 Jurisdictional restrictions

Access from restricted jurisdictions is controlled through a combination of technical, registration-level and operational controls. At the network edge, Cloudflare provides geo-based controls to restrict or manage traffic from blocked territories. In addition, the Company applies jurisdiction controls within the registration flow so that players from excluded jurisdictions are prevented from creating an account or proceeding with use of the site where access is not permitted.

The proprietary front-end and middleware also support additional geo-blocking and eligibility controls. These controls are used to prevent access to restricted products, registration, login, deposits or gameplay where the player's location, selected country of residence, IP location or other relevant account information indicates that access should not be permitted.

The list of accepted and restricted jurisdictions is maintained by the Company and applied through the relevant platform, front-end, middleware and operational configurations. The list is reviewed and updated when market availability, legal requirements, payment availability, provider restrictions or business policy changes require an update.

Players from restricted jurisdictions are prevented from registering or playing on the site, and existing accounts may be restricted where a jurisdictional issue is identified after registration.

6.4 Account monitoring and escalation

Accounts are monitored on an ongoing basis to detect indicators of prohibited or restricted participation. Suspected breaches are escalated through the Company's operational and compliance escalation routes and actioned, including account restriction or closure where appropriate.

7 Technical Infrastructure (LOK Art. 5.9(f))

This section provides an overview of the technical environment supporting the licensed operation.

7.1 Hosting arrangements

The technology stack is fully cloud-hosted on Amazon Web Services (EU) under commercially standard agreements, with no bare-metal or on-premise infrastructure. The Company maintains two distinct AWS environments: a backend/database environment hosting the PAM data and transactional systems, and a front-end/middleware environment hosting the proprietary applications and integrations. The backend environment is managed by the PAM infrastructure teams together with outsourced DevOps/Infrastructure resources; the front-end/middleware environment is managed by in-house engineering together with outsourced DevOps/Infrastructure resources. All AWS accounts are owned and controlled by the Company.

7.2 Server environment

The production cluster runs containerised front-end applications, a middleware service and a CMS service, supported by Redis cache, S3 storage, SQS messaging and an API Gateway. The PAM and transactional data are held in the backend environment, comprising self-managed MySQL on EC2 and AWS RDS.

7.3 Cloud providers

AWS provides the Company's compute, storage, database and messaging services. Cloudflare provides content delivery, web application firewall and DDoS protection at the network edge.

7.4 Network architecture

Production services run inside an AWS Virtual Private Cloud. Player traffic from the brand domains is routed through load balancers to the front-end containers, with the middleware and CMS services orchestrating traffic to data services and external APIs. The backend/database environment is logically isolated from the front-end/middleware environment, reducing blast-radius risk and supporting operational flexibility.

7.5 Monitoring arrangements

Logging is enabled across the infrastructure and application layers where supported and is used for operational troubleshooting and incident investigation. Operational alerting and workflow notifications — including system and service health, transactional and risk-related events, and operational escalations — are orchestrated through the Flows platform. Internet-facing protection and monitoring is provided by Cloudflare. .

7.6 Redundancy measures

The front-end/middleware environment is independently scalable from the backend environment to accommodate traffic variability. Resilience is supported by regular automated backups stored within AWS-managed infrastructure and by the segregation of environments, which limits the impact of operational or security events.

8 Business Continuity and Contingency Arrangements

This section explains how critical operations would continue, or be restored, following operational or technical disruption. Business continuity and disaster-recovery arrangements are maintained proportionate to the Company's scale and risk profile and are supported by the PAM provider and outsourced DevOps/Infrastructure teams.

8.1 Critical operational functions

The functions critical to continuing the licensed operation are player registration and login, deposits and withdrawals, the player wallet and transaction processing, game launch and play, the sportsbook, and customer support. These functions are prioritised in the Company's continuity and recovery arrangements.

8.2 Contingency procedures

A 24/7 incident-management process underpins contingency handling. A single routed out-of-hours number reaches the in house engineer on call for that week, who works the incident through to resolution and triages with the PAM provider and other third parties (for example Altenar and ClamTech) as needed. The PAM provider also operates a 24/7 critical-issue handling process for production incidents.

8.3 Disaster recovery arrangements

Database-level disaster recovery is performed by restoring the most recent recovery-point-compliant AWS Backup restore point to a new EC2 instance, reconfiguring and validating the database, and redirecting application traffic, following the PAM provider's documented restoration procedure. Backups are stored within AWS-managed infrastructure, and the segregation of environments limits the scope of any single failure.

8.4 Recovery responsibilities

Recovery responsibilities are shared and clearly assigned. The weekly on-call engineer owns each incident through to resolution and coordinates the relevant parties. Database restoration is executed by the PAM provider, and the AWS environments are supported by outsourced DevOps/Infrastructure resources. Payment-related issues that cannot be resolved by the PAM provider are escalated to designated senior finance personnel, who can engage the payment service providers directly.

8.5 Communication procedures

During an incident, the on-call engineer posts regular business updates to a critical-issue communication channel, feeds updates to Customer Support and gathers further insight from inbound contacts, and escalates to senior management where required.

8.6 Escalation arrangements

The on-call service-level standard is to answer or call back within 15 minutes. If the on-call number is not answered within 15 minutes, any team member may be called out. The on-call engineer can call out the front-end team, Product Management and senior management as required, and escalate to third parties (the PAM provider, Altenar and ClamTech) through their respective support processes. A current contact and escalation matrix is maintained and reviewed frequently.

8.7 Testing and review

The Company's continuity and recovery arrangements are reviewed periodically, and disaster-recovery procedures are exercised and the results recorded to demonstrate operational resilience.

9 Responsible Gaming (LOK Art. 5.9(g))

This section explains how responsible-gaming principles are implemented throughout the operation, through both automated controls and manual interventions. The framework is owned by the Compliance and Operations functions and is set out in the Company's Responsible Gaming Policy.

9.1 Player protection measures

The Company provides a framework of player-protection measures designed to help players keep control of their play, to identify potentially harmful behaviour, and to intervene where appropriate. These measures are made available through the player interface and are supported by behind-the-scenes monitoring.

9.2 Deposit and loss limits

Players are able to set deposit and loss limits through their account or through customer services. Requests to increase a limit take effect only after the applicable cooling-off behaviour, while reductions take effect promptly, in line with responsible-gaming good practice.

9.3 Time Out and Self-exclusion

Players may apply a Time Out to their account directly through their account settings. During the chosen period, the player will be able to access their account to review account details (such as transaction history) and withdraw any remaining funds while any gambling transactions (such as deposits, placing bets or using bonuses) are suspended. The account will automatically reopen after the chosen Time Out period.

Players may self-exclude for a defined period or on a permanent basis directly through their account settings. Self-exclusion is enforced at the account level, prevents further play and direct marketing for the duration, and is subject to defined reactivation rules at the end of any Self-exclusion period.

Limit, Time Out and Self-Exclusion records are being stored within the PAM.

9.4 Behavioural monitoring

Player activity is monitored for patterns that may indicate at-risk play. Indicators identified through monitoring are reviewed so that the appropriate protective action can be taken.

9.5 Escalation and intervention

Responsible-gaming monitoring triggers both automated controls (such as limit enforcement and prompts) and manual interventions (such as account review, direct contact with the player and, where appropriate, the application of limits or exclusions). Interventions are recorded, and significant cases are escalated through the compliance escalation route.

10 Terms and Conditions (LOK Art. 5.9(h))

This section addresses the Terms and Conditions under which the Company's services are provided to players. The current approved Terms and Conditions are maintained for each brand and published on site.

10.1 Approval process

All changes to the Terms and Conditions, whether minor or substantial, are reviewed and approved by the senior management team before publication. This ensures that any amendment remains accurate, fair and consistent with applicable regulatory requirements. No change to the Terms and Conditions is published until it has been approved through this process.

10.2 Version control

The Terms and Conditions are version-controlled. Each version carries a version number and last-updated date, and prior versions are archived so that the exact wording in force at any given time can be identified. Acceptance of each version is recorded against the player's account in the Company's PAM, including the version accepted and the date and time of acceptance. This provides a complete audit record from which the Company can retrieve which version of the Terms and Conditions applied to a given player at any point in time.

10.3 Review and update

The Terms and Conditions are reviewed periodically, and additionally whenever a change in the business, product or regulatory environment requires an update. Where a change is identified, it is submitted to the senior management team, and once approved the change is implemented and published. All amendments are reported to the Curaçao Gaming Authority at a minimum twice per year, in line with the amendments reporting requirements.

10.4 Alignment with the live site

The Company confirms that the version of the Terms and Conditions referenced in this Manual matches the version currently published and available to players.

10.5 Player Acceptance of updated Terms

Where the Terms and Conditions are materially updated and published on the live site, players are required to review and accept the updated Terms before they can continue using the real-money gaming services. The updated Terms are presented to the player through the website interface after publication, and the player must provide affirmative acceptance before being permitted to proceed with gameplay, deposits, withdrawals or other account activity where acceptance is required.

If a player does not accept the updated Terms, access to real-money play and relevant account functionality is restricted until acceptance is provided. The player may still be directed to customer-support channels where they have questions about the update or require assistance with their account.

Acceptance of updated Terms is recorded against the player account, including the applicable Terms version and the date and time of acceptance, so that the Company can evidence which version of the Terms applied to the player at the relevant time.

11 Complaints and Dispute Resolution (LOK Art. 5.9(i))

This section explains how player complaints and disputes are managed, from submission through to resolution and recordkeeping, consistent with applicable dispute-resolution requirements. It is based on the approved Player Complaint Policy.

11.1 Submission methods

Players can submit complaints via email to the available support email address including the completed complaint form, which is accessible through the terms and conditions in downloadable form. Any complaints received are captured and logged for handling.

11.2 Investigation

Complaints are investigated by the customer support and compliance functions, drawing on account, transaction and gameplay records and, where relevant, information from third-party providers.

11.3 Escalation routes

Complaints that cannot be resolved at first instance are escalated internally to compliance and management. If the player remains dissatisfied with the resolution provided, they may escalate

their complaint to the relevant external dispute resolution body which is clearly described in the terms and conditions.

11.4 Response timeframes

The Company operates target timeframes for acknowledging and resolving complaints, and keeps players informed of progress through to resolution.

11.5 Recordkeeping and oversight

Complaints are recorded in a complaint register, and complaint handling is overseen by management, with trends reviewed so that recurring issues can be addressed.

12 Record Keeping and Retention

This section explains how operational records are maintained throughout the business so that they are complete, retrievable and protected.

12.1 Types of records

The Company maintains the operational records required to evidence how the licensed business is operated. These include player account and registration records, KYC and verification records where applicable, gaming records, financial transaction records, deposit and withdrawal records, responsible-gaming records, complaints and dispute records, customer-support records, operational incident records, supplier and outsourcing records, system access records and audit trails. Records may be held in the PAM, payment systems, reporting tools, customer-support tools, responsible-gaming systems, supplier portals and internal operational repositories, depending on the nature of the record.

12.2 Retention periods and storage

Records are retained for the periods required by applicable gaming, AML and data-protection obligations, in accordance with the Company's retention schedule. The retention schedule identifies the relevant record categories, the applicable retention period and the function responsible for maintaining the record. Records are stored primarily within the AWS environment, the PAM platform and connected operational systems, with environment segregation and access controls as described in Sections 4 and 7. Where records are held by third-party service providers, the Company relies on contractual arrangements and operational access rights to ensure that relevant records remain available when required.

12.3 Retrieval

Records can be retrieved when required through the PAM back office, the Company's reporting tools and the relevant operational systems. Retrieval supports customer-support review, payment reconciliation, investigation of gameplay or transaction queries, responsible-gaming reviews, complaints and dispute handling, AML and fraud investigations, management oversight and regulatory requests. Access to retrieve records is limited to authorised users with a legitimate operational need, and exports are handled in accordance with internal access-control and data-protection requirements.

12.4 Protection against loss or alteration

Records are protected against loss, unauthorised access and unauthorised alteration through role-based access controls, least-privilege permissions, logging, environment isolation, secure system configuration and regular automated backups. Production systems and back-office tools are accessible only to authorised users, and privileged access is restricted and reviewed as described in Sections 4 and 7. Backup and restoration arrangements are described in Sections 8 and 14. Where records are amended as part of normal operations, relevant system logs, audit trails or status histories are retained where supported by the system.

12.5 Responsibility

Responsibility for maintaining each category of record is assigned to the relevant operational, technical, finance, customer-support, responsible-gaming, AML, compliance or management function. System owners are responsible for ensuring that records within their systems are complete and accessible to authorised users. Department heads are responsible for ensuring that their teams follow the applicable record-keeping procedures. Overall oversight is maintained by management, with Compliance supporting regulatory alignment and periodic review of the retention framework.

13 Critical Information and Transaction Records (LOK Art. 5.9(j))

This section should be read together with Section 12. Section 12 describes the Company's general record-keeping and retention framework across the business. This section focuses specifically on the critical player, wallet, gaming, payment and audit records that evidence the operation of the licensed gaming activity and that may be required for regulatory inspection, investigation, reconciliation or reporting purposes.

13.1 Player and account records

Player records are held within the PAM platform, which provides the core player account-management system, with the Company acting as data controller. These records include registration details, contact information, account status, brand, jurisdiction, consents, responsible-gaming settings, verification status where applicable, account restrictions and relevant change history.

Player account activity is available through the PAM back office for authorised users with role-based permissions. This includes sign-ups, logins, conversions, account updates, verification events, status changes, responsible-gaming actions and other account-management events. Records can be searched, filtered by date range and brand, reviewed for operational purposes and exported where required for analysis, investigation or regulatory response.

13.2 Gaming and financial transaction records

Gaming transactions and financial transactions are processed and recorded through the PAM and connected platform components. Gaming records include bets, stakes, settlements, winnings, bonus-related transactions and balance movements. Financial records include deposits, withdrawals, payment status changes, payment-method information where available, failed or pending transactions and related wallet entries.

The PAM-held wallet provides the authoritative record of player balance movements. This ensures that gameplay, payments, settlements and adjustments are recorded against the player account in a consistent transaction history. Deposit and withdrawal records are also processed through the connected payment layer and reconciled through operational and finance processes.

Reporting is provided by the PAM's business-intelligence tool, Acubi. Acubi runs against a separate, logically isolated reporting database that is synchronised from the core PAM databases several times per day. It provides more than one hundred pre-configured reports covering player activity, financial performance, payments, compliance, responsible-gaming, AML, operations and management reporting.

13.3 Audit logs and game history

Logging is enabled across the infrastructure, application and platform layers where supported. Audit trails are maintained for relevant account, system and operational actions, and access to production systems is restricted and logged. These logs support incident investigation, security

review, complaint handling, AML and fraud review, operational troubleshooting and regulatory enquiries.

Game round and game-history data is recorded at the PAM and game-provider level. This includes information required to evidence the game played, the round or transaction reference, stake, result, win amount, settlement and related balance movement. For sportsbook, bet placement and settlement records are maintained through the sportsbook provider and reflected in the PAM transaction history. Game and transaction records are retained in accordance with the Company's retention schedule.

13.4 Regulatory accessibility

Critical information is accessible through the PAM back office, Acubi reporting suite and relevant operational systems for authorised users with role-based permissions. The Company can retrieve and export records required to respond to regulatory requests, including player account records, transaction histories, payment records, game history, responsible-gaming actions, complaints, incidents and audit trails.

Requests from the Regulator are coordinated by the appropriate operational, compliance, finance or technical function, depending on the information requested, with management oversight where required.

14 Data Centre and Hosting Arrangements (LOK Art. 5.9(j))

This section explains where critical information is hosted and stored, and how the hosting model supports protection, availability and recovery of that information. It should be read together with Sections 7, 8, 12 and 13. Those sections describe the wider technical infrastructure, business-continuity arrangements, record-keeping framework and critical transaction records. This section focuses specifically on the hosting and data-centre arrangements that support those records.

14.1 Data Centre and hosting providers

Critical information is hosted in Amazon Web Services cloud infrastructure. The Company does not operate bare-metal servers or on-premise data-centre infrastructure for the licensed gaming operation. The AWS hosting model is used for the production platform, backend/database services, front-end and middleware services, storage, backups and supporting cloud services.

Hosting is organised across two distinct AWS agreements/environments: a backend/database environment and a front-end/middleware environment. The backend/database environment supports the PAM, wallet, transactional systems and related databases. The front-end/middleware environment supports the proprietary websites, middleware, CMS and integrations used to deliver the player-facing experience. All AWS accounts used for the licensed operation are owned and controlled by the Company.

The use of separate backend and front-end environments supports segregation of duties, limits the potential impact of operational or security issues, and helps ensure that critical player, wallet and transaction records are not dependent on a single application layer.

14.2 Redundancy and backup locations

Redundancy is supported by AWS-managed infrastructure, logical separation of the backend/database and front-end/middleware environments, scalable cloud services and regular automated backups. The platform architecture is designed so that the player-facing application layer and the backend transactional layer can be managed, scaled and recovered separately where required.

Backups are stored within AWS-managed infrastructure. Backup vaults, retention policies and access permissions are configured within the managed AWS environment in line with the applicable operational requirements. Core database backups are scheduled at least three times per day, approximately every eight hours, to support the Company's recovery-point objectives.

The backup arrangements are intended to protect critical player account, wallet, transaction and operational records against data loss and to support restoration following a technical incident, system failure or other disruption.

14.3 Restoration capabilities

Restoration is performed in accordance with the applicable PAM provider and infrastructure procedures. Where database restoration is required, the process involves selecting the most recent recovery-point-compliant AWS Backup restore point, restoring it to a new instance, reconfiguring and validating the database, and redirecting application traffic once the restored service has been checked.

Following a restoration event, the Company validates the restored environment and confirms that the relevant application functionality, player account records, wallet balances, transaction history and operational services are functioning as expected. Restoration activities are coordinated between the Company, the PAM provider and the relevant DevOps/Infrastructure

resources, with escalation and communication handled in accordance with the business-continuity procedures described in Section 8.

14.4 Certifications

The Company relies on the compliance certifications and assurance materials of AWS for the underlying cloud infrastructure used to host the production platform, and the PAM provider for backend/database services, storage and backups. These certifications relate to the security, availability and operational controls of the AWS infrastructure layer, while the Company remains responsible for the configuration, access control, monitoring and operation of its own cloud environments and applications.

As mentioned the Company also uses a PCI-approved Approved Scanning Vendor for external vulnerability scanning of internet-facing infrastructure. Vulnerability scan results, remediation records and applicable cloud/data-centre assurance materials are retained as supporting evidence.

14.5 Data-centre tier 4 Curacao considerations

As described in detail in Sections 7 and 14, the Company operates its primary production platform on AWS cloud infrastructure rather than through a single physical data centre. AWS remains the main hosting environment for the PAM, front-end, middleware, wallet, transactional systems and operational platform components.

In addition to the AWS hosting model, the Company is implementing a Curaçao-based data-centre arrangement in response to the local data-hosting and regulatory data-availability requirement expected to apply from July 2026. This arrangement is not intended to replace AWS as the Company's primary production hosting environment. Instead, it will provide an additional Curaçao-based location for defined regulatory data.

The planned arrangement is for selected player and transaction data to be transferred from the PAM to a Curaçao-based Tier 4 data centre by secure SFTP. The data set, transfer frequency, file format, access permissions, monitoring and reconciliation process will be configured in accordance with any applicable regulatory requirements.

The purpose of the Curaçao data-centre transfer is to ensure that the required player and transaction information is available in Curaçao for regulatory access, continuity and oversight purposes, while the live operational platform continues to run in the Company's AWS-hosted production environment.