

OPERATIONS MANUAL

Great Star N.V.

Document Control

Version	Date	Description of Changes	Author
1.0	07.07.2026	Initial draft	IGA Group B.V.

OPERATIONS MANUALOPERATIONS MANUAL

1. PURPOSE

This Operations Manual sets out the operational, technical, compliance, security, and responsible gaming framework implemented by Great Star N.V. in relation to its online gaming operations.

The purpose of this document is to demonstrate the systems, controls, and procedures implemented to ensure compliance with applicable Curaçao Gaming Authority (CGA) requirements, applicable gaming legislation, license conditions, and regulatory obligations.

2. COMPANY INFORMATION

2.1 Legal Entity

Company Name: Great Star N.V.

Registration Number: 122623

Registered Address: Schout Bij Nacht Doormanweg 40, Curacao

Contact Details: s.vogiatzis@gr8star.com

Website(s):

gastonred.com

Sman365.com

Zanzibet.com

Narbi221.com

sharks-bet.com

Gastonred.org

fettibet.com

Turbobet.bet

nacionbet.com

2.2 Key Persons

Position	Name	Contact
Director	eMagnus Curacao B.V.	s.vogiatzis@gr8star.com
CEO	Anastasios Vogiatzis	s.vogiatzis@gr8star.com
MLRO	Ioannis Dalianis	g.dalianis@gr8star.com
CTO	Platform provider's responsibility	N/A
CFO	Anxhela Maloku	a.maloku@gr8star.com

3. DESCRIPTION OF GAMING OPERATIONS

3.1 Games Offered

The Licensee offers online gaming products through approved gaming providers and systems. All gaming content is supplied and operated in accordance with applicable regulatory requirements.

Game Provider	Type of Games
Altenar	Sportsbook
Blue Ocean (aggregator)	Slots / Live Casino / Table Games
Agreegain (aggregator)	Slots / Live Casino / Table Games
Pragmatic Play	Slots / Live Casino / Table Games
Evolution	Slots / Live Casino / Table Games
Hacksaw	Slots
World Match	Slots

3.2 Payment Methods

The Licensee supports the following payment methods:

Deposits

- Credit/Debit Cards
- Bank Transfer
- E-wallets
- Cryptocurrency (where applicable)

Withdrawals

- Bank Transfer
- E-wallets
- Other approved payment methods

All payment processing activities are monitored and performed through approved payment service providers in accordance with applicable AML/CFT requirements.

3.3 Betting Limits

The Licensee applies predefined betting limits to ensure responsible gaming controls and operational integrity.

Product	Minimum Bet	Maximum Bet
Casino	0.05 EUR	10.000 EUR
Sportsbook	0.1 EUR	20.000 EUR

3.4 Payout Procedures

The Licensee applies controlled payout procedures to ensure accurate settlement of gaming transactions.

Winning outcomes are determined through approved gaming systems and settlement procedures. Payout calculations are automatically generated based on the applicable game rules, betting conditions, and approved configurations.

Withdrawals are reviewed and approved through established operational and compliance controls before funds are released.

Applicable payment timelines are communicated to players through the Terms and Conditions and payment information pages.

3.5 Gaming Software

The Licensee operates using approved gaming technology and supporting systems.

System / Service	Provider
Gaming Platform Provider	[AGP and Flexsy]
Sportsbook Provider	[Altenar]
Back-office Systems	[CPP and Taurus]
Certification Laboratories	[Insert Provider]

3.6 Outcome Determination

Gaming outcomes are determined through certified gaming systems and approved random number generation processes.

The Licensee ensures:

- RNG systems operate according to certified methodologies;
- Sportsbook results are settled according to predefined rules;
- Third-party data feeds are obtained from approved providers;
- Game fairness controls are implemented and monitored.

4. QUALITY ASSURANCE AND TESTING

4.1 Testing Schedule

The Licensee performs regular testing and monitoring activities.

Test Type	Frequency	Responsible Person
RNG Testing	Quarterly	Ioannis Dalianis
Penetration Testing	Annually	Ioannis Dalianis
Vulnerability Scanning	Monthly	Ioannis Dalianis
Backup Restoration Test	Quarterly	Ioannis Dalianis

4.2 Quality Monitoring Methods

Quality assurance activities include:

- Internal operational reviews;
- Transaction monitoring;
- Security assessments;
- Software version management;
- Incident monitoring and review procedures.

5. PLAYER DATA MANAGEMENT

5.1 Data Collected

The Licensee collects and processes player information required for account management, regulatory compliance, AML/CFT obligations, and gaming operations.

Collected information includes:

- Name;
- Date of Birth;
- Address;
- Email;
- Phone Number;
- Payment Details;
- Transaction History.

5.2 Data Storage

Player data is stored securely using controlled production databases.

Data security controls include:

- Encryption of data in transit using [];
- Encryption of data at rest using [Insert Standard];
- Secure encryption key management through [Insert Provider/System].

Access to player data is restricted to authorised personnel only.

Access controls include:

- Role-based access management;
- Multi-factor authentication;
- User activity logging.

Player data is retained for the period required by applicable AML/CFT and regulatory requirements.

6. PLAYER INTERFACE

6.1 Website and Application Elements

The Licensee's player interface includes:

- Homepage;
- Registration process;
- Login functionality;
- Responsible Gaming section;
- Deposit and withdrawal pages;
- Bonus information pages.

Relevant screenshots and supporting materials are maintained as part of the licensing documentation package.

6.2 Mandatory Information Displayed

The player interface displays:

- License and company information;
- Responsible Gaming information;
- Terms and Conditions;
- Privacy Notice;
- Complaint handling and dispute resolution information.

7. PLAYER PROTECTION CONTROLS

7.1 Prohibited Players

The Licensee maintains controls preventing access by:

- **Self-excluded players** – Players who have voluntarily excluded themselves or have been excluded by the Licensee are blocked from logging in, creating new accounts, or participating in any gaming activity. Account checks are performed against the self-exclusion register during login and registration;

- **Underage persons** – Age verification procedures are applied at registration and before allowing withdrawals. Players must confirm they meet the minimum legal age requirement, and additional verification checks may be performed using third-party KYC tools;
- **Restricted jurisdictions** – IP detection, country verification, and payment instrument checks are used to prevent access from jurisdictions where services are prohibited or restricted under the applicable licence;
- **Sanctioned individuals** – The Licensee screens players against applicable international sanctions lists using automated compliance tools, and blocks or restricts accounts where a match or potential match is identified in accordance with AML/CFT obligations.

7.2 Verification Controls

Player verification procedures include:

- **KYC verification** – The Licensee applies Know Your Customer procedures at account registration and prior to enabling withdrawals, in order to verify the identity of each player and assess their eligibility to use the services;
- **Identity verification** – Players are required to submit valid identification documents (such as a passport, national ID card, or equivalent) which are checked for authenticity using automated and/or manual verification methods;
- **Age verification** – The Licensee confirms that all players meet the minimum legal age requirement before allowing full account activation or real-money play. Accounts suspected of belonging to underage individuals are suspended pending verification;
- **Enhanced Due Diligence (EDD) procedures where required** – Additional checks are performed on higher-risk players, including source of funds/wealth verification, increased transaction monitoring, and request for supplementary documentation in accordance with AML/CFT obligations.

7.3 Technical Controls

Technical safeguards include:

- **Geolocation monitoring** – The Licensee uses geolocation tools to determine the physical location of players and ensure they are accessing the platform only from permitted jurisdictions. Any inconsistencies between declared and detected locations may trigger further review or access restrictions;
- **IP monitoring** – IP addresses are monitored at login and during gameplay to identify suspicious activity, such as repeated access from restricted countries, use of anonymising services (e.g., VPNs or proxies), or abnormal login patterns;
- **Device fingerprinting** – The Licensee collects device-related information (such as browser type, operating system, device identifiers, and configuration data) to help identify returning users, detect fraudulent behaviour, and prevent misuse of multiple accounts;
- **Duplicate account detection** – Automated systems are used to identify potential duplicate accounts based on shared identifiers such as personal details, device fingerprints, IP addresses, payment methods, and behavioural patterns. Suspected duplicate accounts are reviewed and may be restricted or closed in accordance with the Terms and Conditions.

8. TECHNICAL INFRASTRUCTURE

8.1 Infrastructure Overview

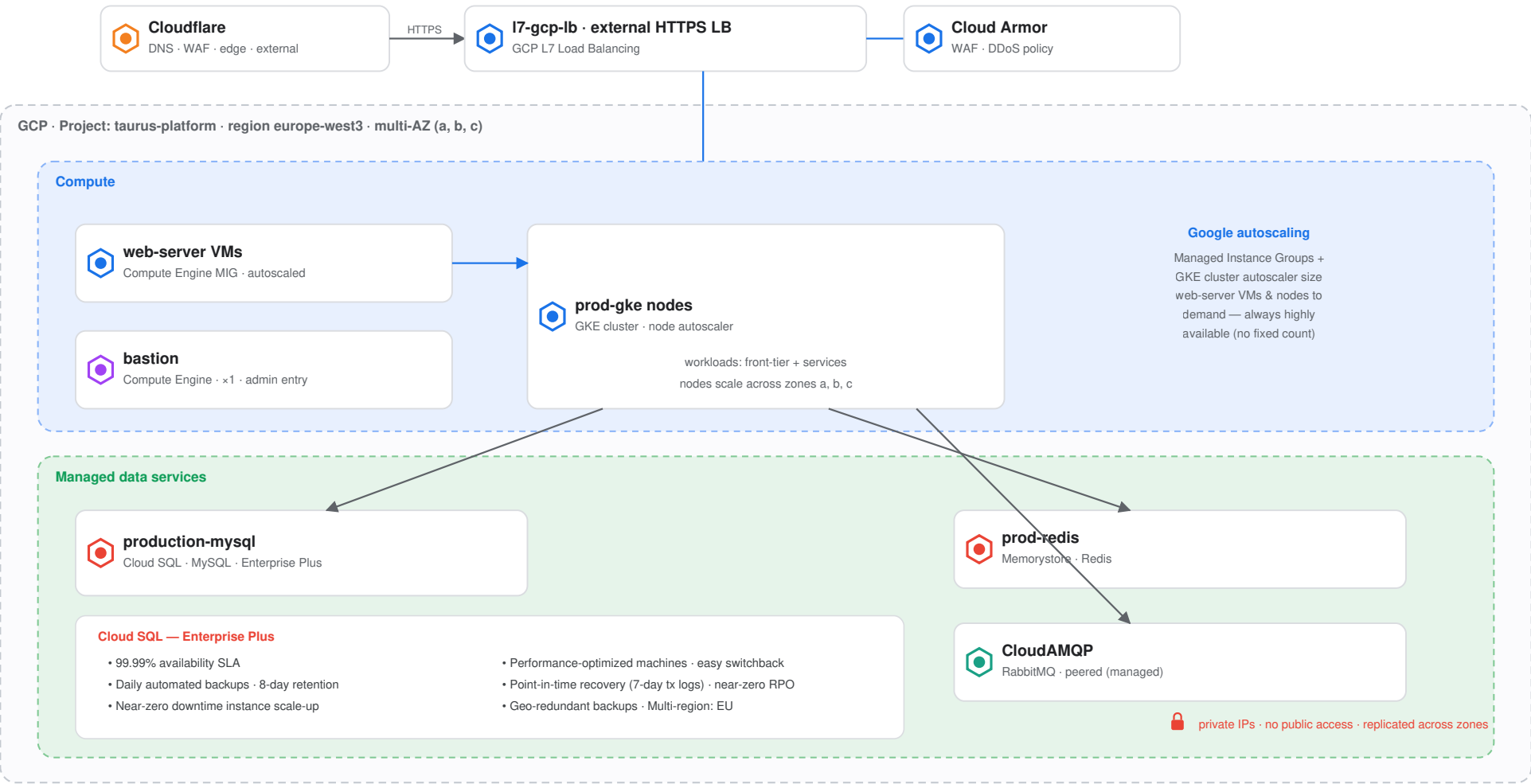
The Licensee maintains documented technical infrastructure including:

- Network architecture;
- Data flow architecture;
- Server infrastructure.

Taurus Platform

Server Infrastructure

Google Cloud Platform (GCP) · 16 July 2026



Compute and managed data services within region europe-west3 — secrets & observability detailed in the notes below.

Ingress & edge

External traffic enters through **Cloudflare** (DNS, WAF, edge) and is routed to the GCP **external HTTPS L7 load balancer** with **Cloud Armor** (WAF / DDoS policy) before reaching compute.

High availability & autoscaling

The number of **web-server VMs and GKE nodes is not fixed** — it is driven by Google's autoscaling mechanisms (**Managed Instance Groups** and the **GKE cluster autoscaler**), which size capacity to demand across **availability zones a, b, c** in region **europa-west3**. This keeps the platform **always highly available**. Managed data services use replicated, zone-redundant configurations.

Cloud SQL — Enterprise Plus (production-mysql)

Runs on **Cloud SQL Enterprise Plus** with a **99.99% availability SLA** and **automated backups**. Key capabilities: **near-zero downtime instance scale-up**, **performance-optimized machines**, **advanced disaster recovery with easy switchback**, and **point-in-time recovery**.

Our Cloud SQL Enterprise Plus database is secured by **daily automated backups retained for 8 days**, establishing a robust baseline for operational recovery. **Point-in-Time Recovery (PITR)** is enabled with **7 days of transaction logs**, allowing us to restore data to any precise second and reducing our **Recovery Point Objective (RPO) to near-zero**. To ensure disaster recovery and strict regulatory compliance, all backups are **geographically redundant** and securely stored across multiple regions within the European Union (**Multi-region: EU**).

Access

The **bastion host** is the only administrative entry point to VMs and GKE nodes. Managed data services expose **private IPs only** — no public access.

Secrets management

HashiCorp Vault stores **application credentials and secrets** — database passwords, API keys and .env values; applications and GKE pods fetch them from Vault at runtime rather than embedding them in images or config. **Data-at-rest encryption keys** are separate and are **managed by Google Cloud** (Google-managed keys, the platform default), not held in Vault.

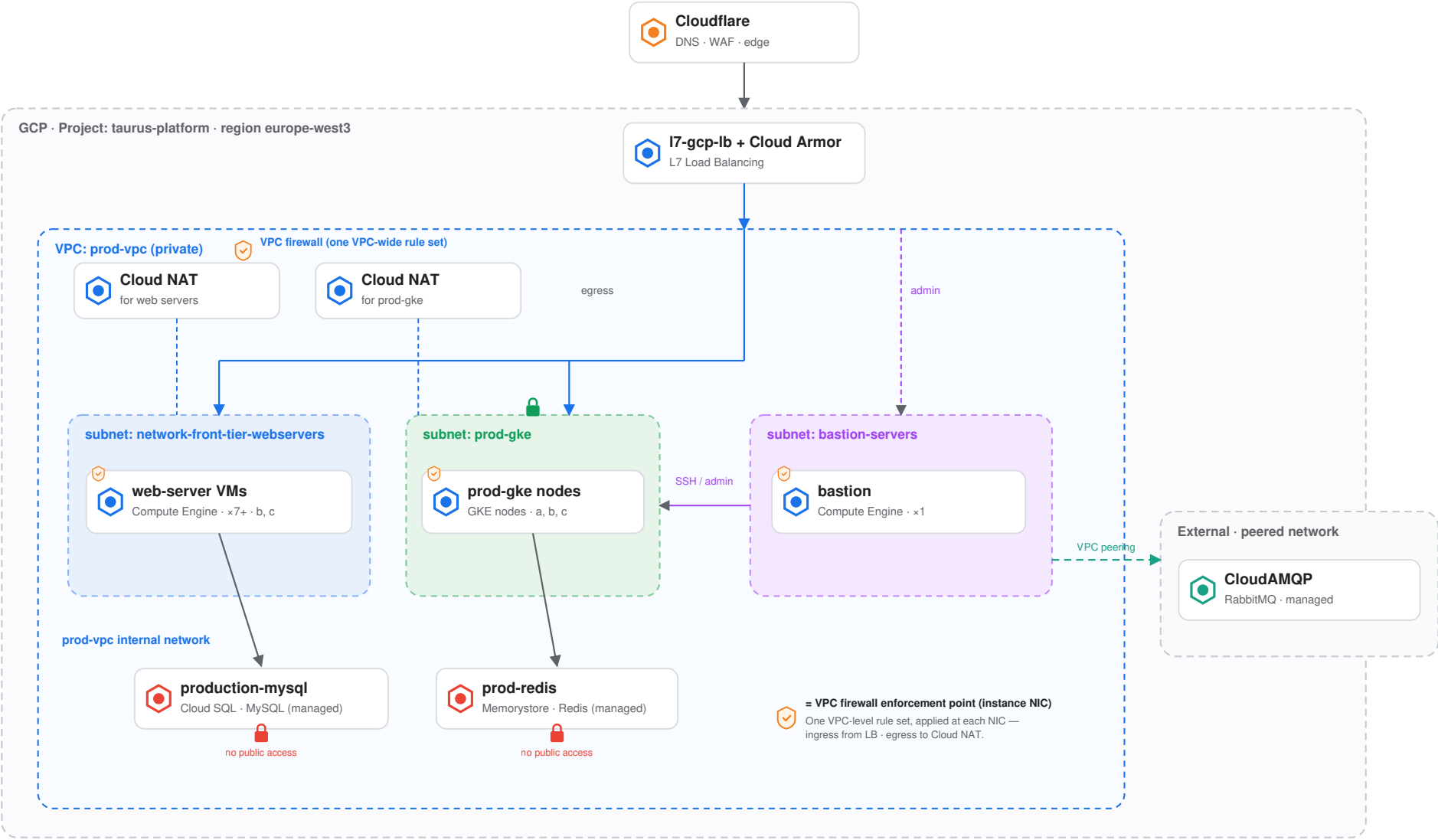
Logging, monitoring & audit

Observability is centralised across **Cloud Logging**, **Cloud Monitoring**, **Prometheus + Grafana** (in-cluster metrics/dashboards) and **audit logs** (admin and data-access auditing).

Taurus Platform

Network Architecture

Google Cloud Platform (GCP) · 16 July 2026



How the network is structured — external actors → Cloudflare → GCP L7 LB → private prod-vpc.

Deployment & region

Production workloads are deployed across **multiple instances and availability zones** within GCP region **europa-west3**, subject to the configuration of each service. Front-tier web VMs and GKE nodes run in multiple zones behind the L7 load balancer for high availability. Capacity is managed by **Google autoscaling mechanisms** (Managed Instance Groups and the GKE cluster autoscaler), which add or remove instances in response to load so that **resources are not maxed out** and the platform stays highly available.

Security boundaries & access controls

- **No public access** to Cloud SQL (production-mysql), Memorystore Redis (prod-redis), GKE nodes or internal VMs. All run on private IPs inside **prod-vpc**; outbound-only egress is via Cloud NAT.
- **VPC firewall rules** are defined once at the **VPC level** and enforced at **each instance's network interface (NIC)** — GCP has no per-subnet firewall appliance. Least-privilege rules (selected by network tags / service accounts) govern **ingress** (e.g. traffic from the L7 load balancer) and **egress** (e.g. outbound via Cloud NAT) for the web-server VMs, GKE nodes and bastion, so only required ports flow between tiers and outbound.
- **Administrative access is restricted through the bastion host**. SSH / admin to GKE nodes and internal VMs is only permitted from the bastion in the bastion-servers subnet; no direct external admin access.
- Ingress is terminated at **Cloudflare** (DNS, WAF, TLS 1.2+) and **Cloud Armor** on the L7 load balancer before reaching the private VPC.
- **VPC peering** to the external CloudAMQP (managed RabbitMQ) network is scoped to required traffic only.

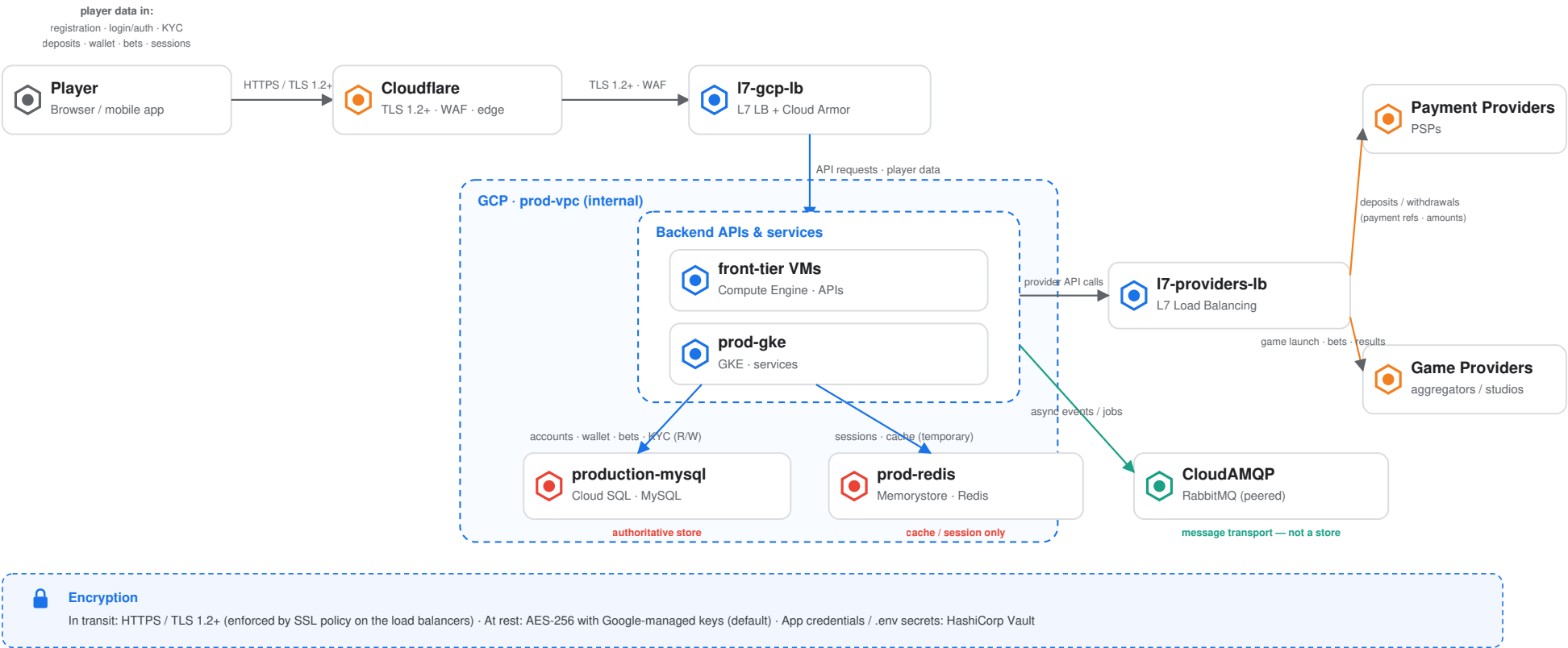
Logging, monitoring & secrets

Observability and audit are centralised via **Cloud Logging**, **Cloud Monitoring**, **Prometheus + Grafana** (in-cluster metrics/dashboards) and **audit logs**. Data at rest is encrypted with **AES-256 using Google-managed keys** (platform default), while **application credentials and secrets** (database passwords, API keys, .env values) are held in **HashiCorp Vault**. See the Server Infrastructure diagram for placement of these services.

Taurus Platform

Data Flow Architecture

Google Cloud Platform (GCP) · 16 July 2026



Player data path across the platform and third-party integrations.

Categories of player data exchanged

The flows above carry the following player-data categories: player registration and profile information; login and authentication data; KYC information (where applicable); deposits and withdrawals; wallet balance and transaction data; betting and gaming activity; game-session tokens; payment status and provider references; and audit and security logs.

Where player data is stored

- **Cloud SQL (production-mysql)** is the **authoritative persistent player database** — accounts, wallet, transactions, bets and KYC records.
- **Memorystore Redis (prod-redis)** stores **temporary cache and session information only**; it is not a system of record.
- **CloudAMQP (RabbitMQ)** handles **messages and events** (transport for async jobs) rather than acting as a permanent player-data repository.
- **Payment and game providers** receive **only the information required for the relevant integration** — e.g. payment references and amounts, or game launch / bet / result data — not the full player record.

Encryption

In transit: connections use HTTPS / TLS 1.2+, enforced by an **SSL policy** on the GCP load balancers. **At rest:** stored data is encrypted at the storage layer with **AES-256**; the encryption keys are **managed by Google Cloud** (Google-managed keys — the platform default). Separately, **application credentials and secrets** (database passwords, API keys, .env values) are stored and brokered through **HashiCorp Vault**, not embedded in application code, images or config.

8.2 Hosting Environment

Component	Location	Provider
Primary Servers	EU-west1 + europe-west3	Google Cloud Platform, Production workloads are deployed across availability zones europe-west3-b and europe-west3-c.
Backup Servers	EU-west1+ europe-west3	Cloud SQL automated backups stored in Google Cloud multi-region eu. Eight automated backups are retained, with point-in-time recovery enabled and seven days of transaction logs retained.
Replication Server	Curaçao	Aquila B.V.

8.3 Security Controls

The Licensee implements and maintains a layered security framework designed to protect systems, data, and player information against unauthorized access, attacks, and misuse. This includes:

- **Firewalls** – Network firewalls are deployed to monitor and control incoming and outgoing traffic based on predefined security rules, ensuring only authorised traffic is permitted;
- **Web Application Firewall (WAF)** – A WAF is used to filter and monitor HTTP/HTTPS traffic between web applications and the internet, helping to prevent common application-layer attacks such as SQL injection and cross-site scripting (XSS);
- **DDoS Protection** – Distributed Denial of Service mitigation tools are in place to detect and absorb malicious traffic spikes, ensuring service availability and platform stability;
- **Access Management Controls** – Role-based access control (RBAC) is implemented to ensure that system and data access is restricted to authorised personnel only, following the principle of least privilege. Multi-factor authentication (MFA) is applied where appropriate for sensitive systems.

8.4 Disaster Recovery

The Licensee maintains documented backup and disaster recovery procedures to ensure business continuity and minimise data loss in the event of a system failure, cyber incident, or other disruptive event. These include:

- **Daily Backups** – Incremental backups of critical systems and databases are performed daily to capture recent changes;
- **Offsite Backup Storage** – Backup data is securely stored in geographically separate offsite environments to protect against localised failures or disasters;
- **Backup Integrity Checks** – Regular verification and testing of backups are performed to ensure data integrity and recoverability;
- **Recovery Procedures** – Defined recovery time objectives (RTO) and recovery point objectives (RPO) are maintained, and periodic disaster recovery tests are conducted to validate readiness.

8.5 Emergency Procedures

The Licensee maintains procedures covering:

- **System failures** – The Licensee has procedures in place to address unexpected system malfunctions, including application errors, software bugs, or infrastructure issues that may affect platform availability or performance. Critical systems are monitored to enable prompt detection, escalation, and recovery actions;
- **Data centre outages** – In the event of a data centre disruption or unavailability, services are designed to be restored through redundant infrastructure and failover mechanisms where applicable. Backup environments and recovery procedures are maintained to minimise downtime and data loss;
- **Cybersecurity incidents** – The Licensee maintains an incident response process to identify, contain, and remediate cybersecurity events such as unauthorised access, malware infections, data breaches, or denial-of-service attacks. Incidents are logged, investigated, and reported in line with internal procedures and regulatory requirements where applicable;
- **Business continuity events** – The Licensee prepares for broader disruptive events such as third-party service outages, critical staff unavailability, power failures, or other operational disruptions. Business continuity plans define roles, responsibilities, and recovery steps to ensure essential services can continue or be restored within acceptable timeframes.

9. RESPONSIBLE GAMING

Responsible Gaming measures are implemented in accordance with the Licensee's Responsible Gaming Policy.

The Responsible Gaming Policy is maintained as a separate controlled document and forms part of the Licensee's compliance framework.

10. TERMS AND CONDITIONS

Player Terms and Conditions governing the use of the gaming platform are maintained as a separate controlled document.

11. PLAYER COMPLAINTS AND DISPUTE RESOLUTION

The Licensee maintains formal complaint handling procedures in accordance with applicable regulatory requirements.

The Complaints Policy is maintained as a separate controlled document.

12. RECORD KEEPING

The Licensee maintains records relating to:

- Player information;
- Gaming activity including bets, wins, losses, and bonuses;
- Deposits, withdrawals, chargebacks, and financial transactions;
- AML/CFT documentation;
- Verification records.

All records are securely stored and retained for a minimum period of five (5) years or longer where required by applicable regulatory obligations.

All required information is available to the Curaçao Gaming Authority upon request through the Licensee's approved technical infrastructure