

# IOGr B.V.

## INFORMATION SECURITY POLICY

Gaming Software Licensor · B2B & Reseller Channel Operations

|                       |                                                            |
|-----------------------|------------------------------------------------------------|
| Document Reference    | ISP-001 — Version 1.0                                      |
| Effective Date        | 01.01.2026                                                 |
| Next Scheduled Review | 01.01.2027                                                 |
| Document Owner        | Chief Information Security Officer                         |
| Classification        | CONFIDENTIAL — Authorised Recipients Only                  |
| Licensing Authority   | Curaçao Gaming Authority (CGA)                             |
| CGA Licence Number    | CGA/2026/1169/1381                                         |
| Company Registration  | 161532 — Curaçao Chamber of Commerce                       |
| Registered Office     | Chuchubiweg 17, Curaçao                                    |
| Director              | Capital Trust Corporation N.V.                             |
| Game Certification    | Gaming Laboratories International (GLI) — GLI-19 Certified |
| Cloud Infrastructure  | Amazon Web Services (AWS)                                  |
| DDoS Protection       | Cloudflare                                                 |
| Key Management        | AWS Key Management Service (AWS KMS)                       |

*This document is the property of IOGr B.V. and contains proprietary and confidential information. Unauthorised disclosure, reproduction, or distribution is strictly prohibited.*

# 1. DOCUMENT CONTROL

## 1.1 Legal Identity

This Policy is issued by IOGr B.V., a private limited liability company incorporated and registered under the laws of Curaçao, with registration number 161532, having its registered office at Chuchubiweg 17, Curaçao, represented by its Director, Capital Trust Corporation N.V..

All game content supplied by the Company to its licensees is certified under the GLI-19 (Online Gaming Systems) standard, independently tested and certified by Gaming Laboratories International (GLI). GLI-19 certification is the foundation of the Company's regulatory compliance and a mandatory condition of its CGA license.

## 1.2 Approval & Sign-Off

| Role                                 | Name                           | Signature | Date |
|--------------------------------------|--------------------------------|-----------|------|
| Director / Authorised Representative | Capital Trust Corporation N.V. |           |      |
| Chief Information Security Officer   | Jason Lee Jr.                  |           |      |
| Data Protection Officer              | Zachary Taylor                 |           |      |
| Head of Legal & Compliance           | Oliver Thomas                  |           |      |
| Money Laundering Reporting Officer   | Alisha Park                    |           |      |

## 1.3 Version History

| Version | Date        | Author                             | Summary of Changes |
|---------|-------------|------------------------------------|--------------------|
| 1.0     | 01.01.02026 | Chief Information Security Officer | Initial issue      |

## 2. INTRODUCTION

### 2.1 Purpose

This Information Security Policy ("Policy") establishes the principles, requirements, and accountability framework that govern how IOGr B.V. ("the Company") protects its information assets, technology infrastructure, game intellectual property, and the data of its authorised licensing partners. The Policy supports the Company's obligations under the Curaçao Gaming Authority (CGA) regulatory framework, applicable data protection law, and internationally recognised security standards.

### 2.2 Business Model

IOGr B.V. operates exclusively as a B2B gaming software licensor. The Company does not operate consumer-facing products, accept player deposits, or hold player funds. The Company licenses its game content and platform technology to third parties under two distinct channel structures:

| Channel                        | Description                                                                                                                                                         | Risk Profile                                                                                       |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Direct Operator (Tier 1)       | A licensed gambling operator that publishes the Company's games directly on its regulated consumer-facing platform, interacting with end-players.                   | High — player data flows through the integration; API is live and player-facing.                   |
| Reseller / Aggregator (Tier 2) | A licensed intermediary that sub-licenses or distributes the Company's games to its own downstream operator network. No direct player interaction with the Company. | Medium — API used for content distribution; downstream operator chain requires ongoing visibility. |

In both cases, the Company is not the Data Controller for end-player personal data. That responsibility rests with the Tier 1 operator running the consumer-facing platform. The Company's obligations as a technology and content licensor are defined in its Data Processing Agreement (DPA) template and Licence Agreement terms.

### 2.3 Policy Objectives

This Policy is designed to:

- Protect the confidentiality, integrity, and availability of all Company systems, source code, game IP, and licensing infrastructure.
- Maintain the demonstrable integrity and fairness of all GLI-19 certified game content supplied to licensees.
- Ensure compliance with Curaçao Gaming Authority requirements and applicable Curaçao and international law.
- Define enforceable security baselines for all Tier 1 and Tier 2 licensees as a condition of license.
- Minimise the risk of API abuse, game manipulation, IP theft, and operational disruption across the licensing channel.

- Establish clear roles, responsibilities, and accountability for information security throughout the Company.

## 2.4 Scope

This Policy applies to:

- All employees, contractors, consultants, and temporary staff of the Company.
- All Tier 1 and Tier 2 licensees, in respect of their obligations under the License Agreement.
- All information systems, networks, APIs, applications, and data assets owned, operated, or managed by the Company.
- All game source code, mathematics documentation, RNG systems, platform APIs, and associated infrastructure.
- All jurisdictions in which the Company holds a license or where its licensees operate under sub-license.

## 2.5 Regulatory & Legal Framework

| Instrument                                                          | Relevance                                                                                                                             |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>CGA — National Ordinance on Offshore Games of Hazard (NOOGH)</b> | Primary licensing framework. Governs game integrity, technical standards, and operator obligations for the Company and its licensees. |
| <b>CGA Technical Standards (current version)</b>                    | Defines RNG certification, game fairness, and platform security requirements.                                                         |
| <b>GLI-19 (Gaming Laboratories International)</b>                   | Certification standard for all IOGr B.V. game titles and RNG systems. Mandatory for all game releases.                                |
| <b>GDPR (EU) 2016/679 / UK GDPR</b>                                 | Applies where the Company processes personal data of EEA or UK data subjects (employee data, licensee contact data).                  |
| <b>AML/CFT Legislation — Curaçao &amp; applicable jurisdictions</b> | Anti-money laundering obligations applicable to the Company's own operations.                                                         |
| <b>ISO/IEC 27001:2022</b>                                           | International ISMS standard to which this Policy is aligned.                                                                          |
| <b>OWASP ASVS/OWASP Top 10</b>                                      | Application security standards mandatory for all Company-developed software.                                                          |
| <b>PCI-DSS v4.0</b>                                                 | Applicable if the Company handles or transmits payment card data in any capacity.                                                     |

## 3. GOVERNANCE & ORGANISATIONAL SECURITY

### 3.1 Roles & Responsibilities

|                                                  |                                                                                                                                                                                                          |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Directo —Capital Trust Corporation N.V.</b>   | Holds directorial authority over IOGr B.V. Bears ultimate accountability for CGA licence compliance and approves this Policy annually. Ensures adequate security resources are allocated.                |
| <b>Chief Information Security Officer (CISO)</b> | Day-to-day ownership of this Policy and the ISMS. Manages the security function, maintains the risk register, oversees audits, and reports quarterly to the Director. Contact: Jason.lee.jr@inout.global |
| <b>Data Protection Officer (DPO)</b>             | Ensures GDPR and applicable data protection compliance. Maintains the RoPA and handles data subject requests. Contact: Zachary.tl@inout.global                                                           |
| <b>CTO/Head of Engineering</b>                   | Owns the secure SDLC, infrastructure security controls, and technical implementation of this Policy.                                                                                                     |
| <b>Money Laundering Reporting Officer (MLRO)</b> | Receives and evaluates internal suspicious activity reports. Manages regulatory AML notifications. Contact: park.Alisha@inout.global                                                                     |
| <b>Head of Legal &amp; Compliance</b>            | Manages licensing obligations, licensee contractual compliance, and regulatory correspondence with the CGA.                                                                                              |
| <b>GLI Liaison</b>                               | Named point of contact for all GLI-19 test submissions, certificate tracking, and renewal scheduling. Contact: <a href="mailto:a.ruiz-ocana@gaminglabs.com">a.ruiz-ocana@gaminglabs.com</a>              |
| <b>All Staff</b>                                 | Must comply with this Policy and all associated procedures. Must report suspected security incidents immediately to the CISO or security@inout.global.                                                   |

### 3.2 Security Steering Committee

The Security Steering Committee (SSC) comprises the CISO, CTO, DPO, MLRO, and Head of Legal & Compliance. It meets quarterly and is responsible for:

- Reviewing and approving updates to this Policy and associated procedures.
- Reviewing the risk register and ensuring treatment actions are progressed on schedule.
- Overseeing significant security incidents and post-incident reviews.
- Approving the annual security roadmap and budget.
- Reviewing penetration test results, audit findings, and GLI-19 certification activities.
- Reviewing the security compliance status of Tier 1 and Tier 2 licensees.

### 3.3 Third-Party & Licensee Risk Management

- A documented risk assessment must be completed for all new licensees and critical vendors before onboarding.
- Tier 1 licensees must pass the Company's Technical Security Onboarding Assessment before receiving production API credentials.
- Tier 2 licensees must complete an enhanced onboarding assessment covering their downstream operator due diligence processes.
- Data Processing Agreements must be executed before any personal data flows between the Company and a licensee.
- Critical technology vendors must provide evidence of ISO 27001 certification or SOC 2 Type II report annually.
- All licensee relationships are reviewed annually by the Head of Legal & Compliance and CISO.

### 3.4 Policy Review Cycle

This Policy is reviewed annually by the CISO, or immediately following a significant security incident, a material CGA regulatory update, or a major change to the Company's technology or business model. All updates require sign-off from the Director (Capital Trust Corporation N.V.) and CISO before reissue.

## 4. ASSET MANAGEMENT

### 4.1 Asset Inventory

A complete and current inventory of all information assets must be maintained, covering hardware, software, AWS cloud resources, game content artefacts, API credentials issued to licensees, and data assets. The inventory is owned by the CISO and reviewed quarterly.

### 4.2 Data Classification Framework

| Level        | Examples                                                                                                                                            | Handling Requirements                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Public       | Marketing materials, published RTP tables, press releases                                                                                           | No restrictions on distribution.                                                                        |
| Internal     | Procedures, project plans, non-sensitive staff communications                                                                                       | Internal circulation only; not shared externally without approval.                                      |
| Confidential | Licensee contracts, employee PII, financial records, integration architecture, audit logs                                                           | Restricted to authorised staff; AES-256 encrypted at rest; TLS 1.3 in transit; access logged.           |
| Restricted   | Game source code, RNG seeds, AWS KMS keys, GLI-19 mathematics documentation and test reports, CGA regulatory submissions, security incident reports | Strictly need-to-know; encrypted; access requires CISO approval; all access events logged in real time. |

### 4.3 Game IP & Source Code Controls

- Version-controlled in the Company's in-house Git repository; access restricted to authorised development staff via RBAC.
- All production commits require at least one peer code review and cryptographic signing before merge.
- Game configuration parameters (RTP, volatility, payable) may only be modified via a formal Change Management process with dual sign-off from Engineering and Compliance. Any change affecting GLI-19 certified parameters must be submitted to GLI for re-certification before deployment.
- Repository access is reviewed and recertified quarterly by the CTO.
- All game build artefacts delivered to licensees must be accompanied by their SHA-256 hash and GLI-19 certificate reference, retained as the authoritative record for CGA audit and dispute resolution.

### 4.4 Licensee Credential Controls

- API credentials and integration tokens issued to licensees are classified Restricted and stored in the Company's self-hosted secrets vault.
- Unique per licensee — credential sharing between licensees is strictly prohibited.
- Rotated every 12 months as standard and immediately upon any suspected compromise.

- Revoked within 4 business hours of contract termination, regulatory suspension, or breach notification.
- All issuance, rotation, and revocation events are logged in the audit trail.

## 4.5 Asset Disposal

Hardware undergoing disposal must be securely wiped per NIST SP 800-88 (Clear or Purge) or physically destroyed. A destruction certificate must be retained for 5 years. AWS storage assets must be securely deleted using AWS-certified deletion procedures prior to resource termination.

## 5. ACCESS CONTROL & IDENTITY MANAGEMENT

---

### 5.1 Core Principles

Access to all Company systems and data is governed by least privilege, need-to-know, and separation of duties. Access rights are reviewed and recertified quarterly by system owners.

### 5.2 Role-Based Access Control

- Every user account must be linked to a defined role with documented access permissions.
- Access must be formally requested, approved by the system owner, and recorded before provisioning.
- Access must be revoked within 24 hours of employment termination or a role change.
- Shared or generic accounts are prohibited in all production environments.
- Service accounts must be non-interactive, scoped to minimum required permissions, and reviewed quarterly.

### 5.3 Privileged Access Management

Privileged access is managed through Google Workspace and Google Cloud IAM. Controls include:

- All privileged accounts (system administrators, DevOps, database administrators, AWS console access) are provisioned and governed through Google Cloud IAM with policy-bound role assignments.
- Just-in-time (JIT) access is enforced for production system access via Google Cloud IAM Conditions and AWS IAM role assumption with time-bound session tokens.
- All privileged sessions must be recorded and retained for a minimum of 12 months.
- Privileged access to game configuration systems requires dual authorisation — two named individuals must approve before access is granted.
- Emergency break-glass access procedures are documented, logged, and reviewed by the CISO within 24 hours of use.

### 5.4 Multi-Factor Authentication

MFA is mandatory for all access to Company systems without exception:

- All staff accounts — Google Workspace, AWS Console, VPN, source code repositories.
- All licensee access to the operator portal and API management console.
- All remote access to internal infrastructure via the self-hosted VPN solution.

Accepted MFA methods: Google Authenticator (TOTP) or FIDO2/WebAuthn hardware security keys. SMS-based OTP is not permitted for any privileged or production access.

### 5.5 Licensee Portal & API Access Controls

- Each Tier 1 and Tier 2 licensee receives a unique, isolated credential set scoped to their contracted game portfolio and markets; stored in the self-hosted secrets vault.

- Licensee portal access is subject to MFA and IP allowlisting enforced at the Cloudflare layer.
- Tier 2 API access is scoped to content catalogue and distribution functions only; Tier 2 licensees have no access to end-player transaction data.
- Licensee accounts are reviewed and recertified annually as part of the licence renewal process.
- The Company reserves the right to suspend API access immediately where a security risk is identified.

## 5.6 Password Standards

| Parameter        | Standard                                                                                                                                                     |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Minimum Length   | 16 characters (standard accounts); 24 characters (privileged accounts).                                                                                      |
| Complexity       | Must include uppercase, lowercase, numeric, and special characters. Common passwords and dictionary words are rejected at the Google Workspace policy layer. |
| Expiry           | Privileged accounts: 90 days. Standard accounts: on suspected compromise only (per NIST SP 800-63B).                                                         |
| Reuse Prevention | Last 15 passwords must not be reused (enforced by Google Workspace).                                                                                         |
| Storage          | Argon2id primary; bcrypt or scrypt acceptable. MD5 and SHA-1 are strictly prohibited.                                                                        |
| Sharing          | Credential sharing between individuals is strictly prohibited.                                                                                               |

## 6. GAME INTEGRITY & ANTI-TAMPERING

### 6.1 GLI-19 Certification Programme

All game content and RNG systems supplied by IOGr B.V. are certified under the GLI-19 (Online Gaming Systems) standard by Gaming Laboratories International (GLI). This certification is a non-negotiable requirement for all titles released to production and a condition of the CGA license.

| GLI-19 Requirement           | Detail                                                                                                                                                                                |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Testing Laboratory</b>    | Gaming Laboratories International (GLI)                                                                                                                                               |
| <b>Applicable Standard</b>   | GLI-19: Standard for Online Gaming Systems (current version)                                                                                                                          |
| <b>Certification Scope</b>   | All RNG systems, game mathematics, payable accuracy, RTP verification, and game logic for every game title released to licensees.                                                     |
| <b>Renewal Triggers</b>      | Any material change to game mathematics, RNG configuration, RTP, or payable data. Also renewed per CGA technical standards schedule or on CGA request.                                |
| <b>Certificate Retention</b> | All GLI-19 test reports and certificates retained for a minimum of 5 years; available to the CGA within 24 hours of a written request.                                                |
| <b>Licensee Disclosure</b>   | Each game build delivered to a licensee must reference its GLI-19 certificate number. Licensees must not deploy a build for which a valid, current GLI-19 certificate does not exist. |
| <b>GLI Liaison</b>           | The designated GLI Liaison manages all test submissions, certificate tracking, and renewal scheduling (see Section 3.1).                                                              |

### 6.2 RNG Integrity Controls

- RNG seed material is generated from a hardware-based cryptographically secure entropy source and stored as Restricted data under AWS KMS.
- RNG output logs are retained in an immutable, write-once format for a minimum of 5 years, available for CGA audit within 24 hours.
- RNG system access in production is restricted to a named list of personnel approved by the CISO; all access events are logged.
- Any deviation between live RNG output and the GLI-19 certified RNG configuration is treated as a P1 security incident — the CISO, Head of Compliance, and GLI Liaison must be notified immediately.

### 6.3 Game Build Integrity

- All production builds are compiled only from tagged, reviewed, GLI-19 certified releases in the in-house repository.

- Every build artefact delivered to a licensee must be accompanied by its SHA-256 hash, digital signature, and GLI-19 certificate reference. The hash and certificate reference together constitute the authoritative production record.
- Any change to game mathematics, RTP, paytable, or volatility must follow the Change Management Procedure with dual sign-off from Engineering and Compliance before GLI submission and before deployment.
- Licensees detecting a discrepancy between the deployed build and its published hash or certificate reference must notify the Company within 24 hours.

## 6.4 Anti-Cheat & Abuse Prevention

- The in-house platform implements server-side behavioural analytics to detect and flag automated play, coordinated bonus abuse, and pattern-based manipulation.
- Rate-limiting and request throttling are applied at the Cloudflare edge layer and at the API gateway for all game-play and wallet-interaction endpoints.
- Anomaly detection rules are reviewed and updated at minimum quarterly by the security team.
- Where abuse is detected on a licensee integration, the Company will notify the licensee and may suspend the affected credentials pending investigation.

## 6.5 Tamper-Evident Audit Logging

- Every game round, spin, bet, outcome, and settlement event must be logged with a unique transaction ID, UTC timestamp, game identifier, game version hash, GLI-19 certificate reference, and session token.
- Game logs are write-once and stored in a tamper-evident in-house log store with cryptographic chaining.
- Logs are reconcilable against financial settlement data from Tier 1 licensees; discrepancies must be investigated within 4 hours of detection.
- Game logs are retained for 5 years and available for CGA or GLI audit within 24 hours.

## 6.6 Internal Manipulation Controls

- Separation of duties: no single individual may both modify game configurations in production and approve that same change.
- All production game configuration changes require dual authorisation and generate an immutable audit entry in the in-house audit log.
- The Company's whistleblowing policy provides a confidential channel for staff to report suspected game manipulation, RNG tampering, or internal fraud.

## 7. SOFTWARE DEVELOPMENT & SECURE SDLC

### 7.1 Secure Coding Standards

- OWASP Top 10 — all web-facing applications are tested against the current OWASP Top 10 risk list.
- OWASP ASVS Level 2 — minimum verification standard for all applications handling licensee or business data.
- CWE Top 25 — most dangerous software weaknesses must be actively identified and mitigated.
- Company Secure Coding Guidelines (ref: SCG-001) — mandatory for all development staff.

### 7.2 Code Review

- All changes to production systems must receive at least one peer review before merge.
- Security-sensitive code paths (authentication, API signing, game logic, RNG integration) require review by a security-qualified senior engineer.
- Code review records are retained as part of the development audit trail for 3 years.

### 7.3 Application Security Testing

| Activity                         | Tooling / Approach                                                                                                                              | Frequency                   |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| <b>SAST (Static Analysis)</b>    | In-house tooling integrated into the CI/CD pipeline. No Critical or High findings may be merged without CISO-approved exception.                | Every pull request          |
| <b>DAST (Dynamic Analysis)</b>   | In-house dynamic analysis against staging environment.                                                                                          | Pre-release and quarterly   |
| <b>SCA (Dependency Scanning)</b> | In-house SCA tooling scanning all third-party libraries for known CVEs.                                                                         | Every CI/CD pipeline run    |
| <b>Container Image Scanning</b>  | Trivy (in-house deployment) scanning all images before push to the production registry.                                                         | Every build                 |
| <b>Penetration Testing</b>       | External CREST-accredited or equivalent third-party firm. Scope: all internet-facing systems, API endpoints, operator portal, internal network. | Annually; pre-major release |
| <b>Responsible Disclosure</b>    | In-house programme hosted at [DISCLOSURE URL]. Acknowledgement within 3 business days; remediation timeline within 7 business days.             | Ongoing                     |

## 7.4 Environment Separation

- Development, staging, and production environments are strictly separated at the network level within AWS using separate VPCs and accounts.
- Real licensee data must never be used in development or staging. Synthetic or anonymised data must be used.
- Production credentials and RNG seeds are never accessible from development or staging environments.

## 7.5 CI/CD Pipeline Security

- All pipeline runs are authenticated via the in-house CI/CD system; anonymous executions are not permitted in production workflows.
- Pipeline secrets are stored in the self-hosted secrets vault and injected at runtime — never baked into container images or committed to the repository.
- Build artefacts are signed before deployment; signatures are verified by the pipeline before promotion to production.
- All deployments to production require approval from at least two authorised individuals (four-eyes principle).
- Pre-commit hooks scan all commits for inadvertent secrets, credentials, or PII.

## 7.6 Dependency & SBOM Management

- A Software Bill of Materials (SBOM) in SPDX or CycloneDX format is maintained for all production applications and updated with each release.
- All third-party libraries are sourced from official, trusted repositories only.
- Critical vulnerabilities (CVSS 9.0+): patch or apply documented mitigating control within 24 hours.
- High vulnerabilities (CVSS 7.0–8.9): patch within 7 calendar days.

## 8. NETWORK & INFRASTRUCTURE SECURITY

---

### 8.1 Infrastructure Overview

The Company's production infrastructure is hosted on Amazon Web Services (AWS). Network security is layered across the Cloudflare edge, AWS-native controls, and the in-house application stack. The self-hosted VPN solution controls all remote administrative access.

### 8.2 Network Segmentation

The AWS environment must be divided into controlled VPC segments with explicit security group and NaCL rules between them. Minimum required zones:

- DMZ / Edge — Cloudflare-fronted internet-facing services: game API delivery, licensee portal, integration webhooks.
- Application Zone — Game platform backend, wallet bridge services, internal application servers.
- Data Zone — AWS RDS / database instances, game log stores, S3 data stores, backup systems.
- Management Zone — Administrative access, monitoring, AWS Security Hub, security tooling.
- Development Zone — Separate AWS account; no VPC peering to production data or credentials.

### 8.3 Firewall & Perimeter Controls

- All internet-facing services are fronted by Cloudflare (WAF, DDoS mitigation, and edge security). AWS Security Groups provide a second-layer default-deny perimeter.
- Inbound rules operate on a default-deny policy at both the Cloudflare and AWS Security Group layers.
- AWS Security Group rule sets are reviewed quarterly and following any significant infrastructure change.
- Outbound traffic from production instances is restricted to known, required destinations via AWS Security Group egress rules.

### 8.4 DDoS Protection

All internet-facing services — game delivery endpoints, licensee portal, and B2B APIs — are protected by Cloudflare's volumetric and application-layer DDoS mitigation. Controls include:

- Cloudflare DDoS protection is active on all proxied DNS records covering game API, licensee portal, and integration endpoints.
- Cloudflare WAF rulesets are maintained and reviewed quarterly; custom rules are added in response to observed attack patterns.
- DDoS response runbooks are maintained and tested annually.
- Cloudflare traffic analytics are monitored continuously; anomalous traffic volumes trigger automated alerting.

## 8.5 Cloud Security — AWS

- All AWS environments are configured in accordance with the CIS AWS Foundations Benchmark (Level 2 for production; Level 1 for staging and development).
- AWS Security Hub is the Company's primary CSPM tool, continuously monitoring for misconfigurations, CIS benchmark deviations, and AWS Foundational Security Best Practice violations.
- All AWS S3 buckets and RDS instances must have public access blocked; any exception requires written CISO approval and is reviewed monthly.
- Separate AWS accounts are used for development, staging, and production environments.
- AWS CloudTrail is enabled in all regions and accounts; all management and data events are logged and forwarded to the in-house SIEM.
- AWS infrastructure is defined and deployed as code (IaC); all IaC templates are scanned for security misconfigurations before deployment.

## 8.6 Secrets Management

The Company operates a self-hosted secrets management vault (HashiCorp Vault) for all application secrets, API credentials, database passwords, and service account tokens:

- All secrets are injected into applications at runtime via Vault dynamic secrets or static secret injection — never baked into container images or stored in the code repository.
- Vault is deployed in high-availability configuration within the AWS management zone.
- All secret access events are logged and forwarded to the in-house SIEM.
- Vault unsealing keys are held by at least two named custodians; no single individual holds sole unseal capability.

## 8.7 Key Management — AWS KMS

AWS Key Management Service (AWS KMS) is the Company's primary key management system for all encryption keys:

- All AWS KMS customer-managed keys (CMKs) are used for encryption of S3 data, RDS databases, EBS volumes, and game log stores.
- Key policies restrict key usage to authorised IAM roles only; no cross-account key sharing without explicit approval.
- Automatic key rotation is enabled for all applicable CMKs on a 12-month cycle.
- KMS key usage events are logged via CloudTrail and monitored by the in-house SIEM for anomalous access patterns.
- RNG seed encryption uses a dedicated, access-restricted KMS CMK; access requires CISO approval and generates an immediate SIEM alert.

## 8.8 Secure Remote Access

All remote administrative access to Company systems is via the Company's self-hosted VPN solution:

- The self-hosted VPN is the sole authorised method for remote access to AWS production infrastructure and internal systems.
- MFA (Google Authenticator TOTP or FIDO2 key) is enforced for all VPN authentication.

- VPN sessions time out automatically after 30 minutes of inactivity.
- VPN access is restricted by user role; production access requires a separate privileged VPN profile approved by the CISO.
- All VPN connection events are logged and forwarded to the in-house SIEM.

## 8.9 Game Content Delivery

- Game assets delivered via CDN are integrity-protected using Subresource Integrity (SRI) hashes; Cloudflare is used for CDN edge delivery.
- Cloudflare configurations enforce licensee-specific allowlists and geo-restrictions consistent with CGA licensing obligations.
- Cloudflare access and delivery logs are retained for 12 months and monitored for anomalous patterns.

## 9. DATA PROTECTION & PRIVACY

### 9.1 The Company's Role

IOGr B.V. is a B2B game licensor and does not operate consumer-facing gambling products. The Company does not collect, store, or process end-player personal data in the ordinary course of its business.

The Company acts as:

- Data Controller — for personal data of its own employees, contractors, and authorised personnel of its licensee organisations.
- Data Processor — in limited circumstances where a Tier 1 licensee contractually instructs the Company to process a defined category of player data (e.g. game dispute resolution). Such processing occurs only within the scope of documented written instructions and a signed DPA.

### 9.2 Data Processing Agreements

- A DPA must be signed before any personal data is shared between the Company and a licensee.
- Sub-processor arrangements must be disclosed to licensees; new sub-processors for licensee data require licensee approval before engagement.
- All DPAs must include provisions for breach notification, audit rights, and data deletion upon contract termination.

### 9.3 Employee & Contact Data

- Personal data of employees and licensee contacts is collected only to the extent necessary for the employment or business relationship.
- A Record of Processing Activities (RoPA) is maintained by the DPO and reviewed annually.
- Data subject rights requests must be acknowledged within 3 working days and fulfilled within 30 calendar days.
- Employee PII is encrypted at rest via AWS KMS (AES-256) and in transit via TLS 1.3.

### 9.4 Data Retention Schedule

| Data Category                      | Retention Period                                   | Basis                                              |
|------------------------------------|----------------------------------------------------|----------------------------------------------------|
| Employee HR records                | Employment + 7 years                               | Legal and contractual obligation                   |
| Licensee contract records          | Contract duration + 7 years                        | CGA audit readiness; commercial records            |
| Game outcome / transaction logs    | 5 years from event date                            | CGA technical standards; GLI-19 audit requirements |
| GLI-19 test reports & certificates | 5 years from certificate date                      | CGA regulatory obligation; licensee audit rights   |
| Security and audit logs            | 12 months hot (SIEM);<br>3 years cold (S3 Glacier) | ISO 27001 / operational security                   |

|                          |                                       |                                              |
|--------------------------|---------------------------------------|----------------------------------------------|
| AWS CloudTrail logs      | 12 months hot; 3 years archived in S3 | AWS security monitoring; CGA audit readiness |
| API access logs          | 12 months                             | Security monitoring; dispute resolution      |
| Penetration test reports | 3 years                               | Regulatory audit readiness                   |
| Incident records         | 5 years                               | CGA regulatory obligation; legal risk        |

## 9.5 Data Breach Response

Where a breach involves personal data of EEA or UK data subjects likely to result in a risk to individuals' rights, notification to the relevant supervisory authority must be made within 72 hours (GDPR Art. 33). Licensee Data Controllers must be notified within 24 hours where their integration data is involved.

## 9.6 International Transfers

Transfers of personal data of EEA or UK data subjects outside those territories must be protected by Standard Contractual Clauses (SCCs), an adequacy decision, or binding corporate rules as applicable under GDPR Chapter V.

## 10. API & INTEGRATION SECURITY

---

### 10.1 Authentication & Authorisation

- All B2B APIs require authentication via OAuth 2.0 with PKCE (interactive flows) or API key with HMAC-SHA256 request signing (server-to-server). API credentials are issued from the self-hosted secrets vault.
- API keys are transmitted exclusively over TLS 1.3 and must never appear in URL query strings or access logs.
- API keys are rotated every 12 months and immediately upon any suspected compromise.
- Requests are authorised against the licensee's contracted scope at the API gateway layer; out-of-scope requests are rejected with HTTP 403.

### 10.2 API Security Controls

- Per-key and per-IP rate limiting is enforced at the Cloudflare edge and at the in-house API gateway layer.
- All inputs are validated and sanitised server-side; client-side validation does not constitute a security control.
- API error responses must not disclose stack traces, database schema, or internal system information.
- API versioning is maintained; breaking changes require a minimum of 90 days' advance written notice before deprecation.
- Webhook payloads are signed with HMAC-SHA256; licensees must verify the signature before processing.
- All API calls must be idempotent or carry idempotency keys to prevent duplicate game round settlements.

### 10.3 Tier 1 Integration Requirements

- Tier 1 licensees must complete the Company's Technical Security Onboarding Assessment before receiving production credentials.
- Integration must use the Company's published API specification; undocumented patterns are not permitted.
- Tier 1 licensees must notify the Company immediately, and within 4 hours at most, upon suspecting credential compromise.
- Tier 1 licensees must maintain TLS 1.2 or 1.3 on their own receiving endpoints.

### 10.4 Tier 2 Integration Requirements

- Tier 2 licensees receive a restricted credential set scoped to content catalogue and distribution functions only, issued from the self-hosted vault.
- Tier 2 licensees must document their downstream operator network and update the Company within 5 business days of any change.

- Tier 2 licensees must flow down the minimum-security requirements of this Policy to downstream operators via their sub-licence agreements. The Company's Licensee Security Schedule (LSS-001) is the minimum acceptable baseline.
- The Company reserves the right to audit a Tier 2 licensee's downstream operator list and sub-licence security terms on 10 business days' written notice.

# 11. FINANCIAL SECURITY & REVENUE SETTLEMENT

---

## 11.1 Revenue & Royalty Settlement

IOGr B.V. does not hold player funds. Revenue is derived from royalties and licensing fees paid by licensees. Financial security controls focus on the integrity of settlement data flows and protection of Company financial systems.

- All royalty settlement data from licensees must be reconciled against the Company's own game transaction logs within 5 business days of the settlement period close.
- Discrepancies exceeding 0.5% of submitted GGR must be escalated to the CFO and CISO within 2 business days.
- Invoicing and payment systems are access-controlled and segregated from game operation systems within AWS.
- No single individual may both approve royalty calculations and authorise payment.

## 11.2 Fraud Detection in Revenue Flows

- Automated monitoring is in place within the in-house analytics platform to detect anomalous licensee settlement patterns.
- Flagged anomalies must be reviewed by Finance and Compliance within 3 business days.
- Suspected deliberate misreporting must be notified to the MLRO, who will initiate a formal investigation.

## 11.3 Payment Security

Where the Company processes payment card data (e.g. for direct licensee invoicing), PCI-DSS v4.0 compliance at the applicable merchant level is mandatory. Card data must not be stored unless essential; if stored, it must be encrypted via AWS KMS, tokenised, and held in a PCI-DSS certified environment.

## 12. CRYPTOGRAPHY

### 12.1 Encryption Standards

| Use Case                                     | Standard & Implementation                                                                                                                                         |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data at rest (databases, S3, backups)</b> | AES-256-GCM via AWS KMS customer-managed keys (CMKs). Applies to all Confidential and Restricted data.                                                            |
| <b>Data in transit</b>                       | TLS 1.3 preferred; TLS 1.2 minimum. Enforced at the Cloudflare edge and at all internal service-to-service endpoints. SSLv3, TLS 1.0, and TLS 1.1 are prohibited. |
| <b>Password/credential storage</b>           | Argon2id primary; bcrypt or scrypt acceptable with current work factors. MD5 and SHA-1 are prohibited.                                                            |
| <b>Game build signing</b>                    | RSA-4096 or ECDSA P-384 minimum, using keys stored in the self-hosted secrets vault.                                                                              |
| <b>API request signing</b>                   | HMAC-SHA256 minimum. Keys issued from the self-hosted secrets vault.                                                                                              |
| <b>RNG seed protection</b>                   | AES-256 at rest under a dedicated, access-restricted AWS KMS CMK; consistent with GLI-19 RNG security requirements.                                               |

### 12.2 Key Management — AWS KMS

- All cryptographic keys for data encryption are managed through AWS KMS using customer-managed keys (CMKs).
- Key rotation is automated within AWS KMS on a 12-month cycle for symmetric CMKs.
- Asymmetric signing keys (game builds, API signing) are held in the self-hosted secrets vault; rotated every 24 months or on compromise.
- Compromised or lost keys must be revoked immediately; a P1 security incident must be raised.
- KMS key policies enforce least-privilege access; key usage is logged via CloudTrail and monitored by the in-house SIEM.

### 12.3 Secrets Management — Self-Hosted Vault

- All application secrets, API credentials, database passwords, and service tokens are stored in the self-hosted HashiCorp Vault, deployed in HA configuration within the AWS management VPC.
- Secrets are injected into applications at runtime via Vault agent or dynamic secret generation — never stored in container images, IaC templates, or the code repository.
- Automated pre-commit hooks scan all commits for inadvertent secrets; any detected commit triggers immediate rotation and a security review.
- Vault unsealing keys are split across at least two named custodians using Shamir's Secret Sharing.

### 12.4 TLS Certificate Management

- External TLS certificates are issued and renewed through Cloudflare (managed certificates) or a publicly trusted CA for services not fronted by Cloudflare.
- A certificate inventory is maintained with automated 30-day pre-expiry alerting.
- Certificates with RSA key lengths below 2048-bit or SHA-1 signatures must not be used.
- Certificate Transparency (CT) logging is enabled for all public certificates; CT log anomaly monitoring is in place.

## 13. ENDPOINT & DEVICE SECURITY

### 13.1 Endpoint Protection

All Company-managed endpoints operate a standardised in-house managed security configuration (EDR, host-based firewall, and OS hardening baseline) enforced via the Company's device management policy. The in-house security team monitors endpoint alerts.

- EDR alerts are triaged within 2 hours during business hours and 4 hours outside business hours.
- Endpoints not compliant with the security baseline are blocked from accessing Company networks via VPN policy enforcement.

### 13.2 Patch Management SLAs

| CVSS Score | Severity | Remediation SLA                                               |
|------------|----------|---------------------------------------------------------------|
| 9.0 – 10.0 | Critical | Patch or apply documented mitigating control within 24 hours. |
| 7.0 – 8.9  | High     | Patch within 7 calendar days.                                 |
| 4.0 – 6.9  | Medium   | Patch within 30 calendar days.                                |
| 0.1 – 3.9  | Low      | Patch at next maintenance window; maximum 90 days.            |

End-of-life software and OS versions no longer receiving security updates must not be used in production. A remediation plan must be in place within 30 days of EOL notification.

### 13.3 Mobile & BYOD Policy

- All Company-issued mobile devices operate under the in-house device management policy, enforcing screen lock, full-disk encryption, and remote wipe capability.
- Personal (BYOD) devices may only access Company systems via a containerised profile that separates Company and personal data; access is gated through the self-hosted VPN.
- BYOD devices must run a supported OS version with current security patches.
- Access to Restricted class data from BYOD devices requires CISO approval.

## 14. INCIDENT RESPONSE & BUSINESS CONTINUITY

### 14.1 Incident Classification

| Severity | Label    | Examples                                                                                                                             | Response SLA                                                                                                                                                                          |
|----------|----------|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| P1       | Critical | Confirmed data breach; ransomware; game or RNG compromise; platform-wide API outage; GLI-19 certification breach; CGA licence breach | Immediate — within 1 hour. CISO, CTO, MLRO, Director (Capital Trust Corporation N.V.) notified. CGA notification assessed within 4 hours. GLI notified if game integrity is affected. |
| P2       | High     | Suspected breach; active DDoS bypassing Cloudflare; API credential compromise; significant fraud; multi-licensee API degradation     | Within 4 hours. CISO and CTO notified.                                                                                                                                                |
| P3       | Medium   | Isolated malware; access control failure; single licensee API issue; suspicious insider activity                                     | Within 24 hours. Security team lead notified.                                                                                                                                         |
| P4       | Low      | Policy violation; unsuccessful attack; minor misconfiguration; failed brute-force                                                    | Within 5 business days.                                                                                                                                                               |

### 14.2 Incident Response Process

1. Detection & Reporting — Any staff member suspecting an incident must report immediately to security@inout.global. All incidents are logged with a unique reference.
2. Triage & Classification — The on-call security engineer triages and assigns severity within 30 minutes of receipt.
3. Containment — Immediate actions: isolating AWS resources, revoking credentials in the self-hosted vault, activating Cloudflare under attack mode, or suspending licensee API access as appropriate.
4. Investigation — Forensic investigation to establish root cause, attack vector, affected AWS resources, and impact scope. AWS CloudTrail, VPC Flow Logs, and SIEM data used as primary evidence sources.
5. Eradication — Threat removed; affected systems restored from verified AWS backups with integrity confirmed.
6. Recovery — Systems returned to production with enhanced monitoring. Licensees notified under contractual notification obligations.
7. Regulatory Notification — CGA notification assessed within 4 hours of a P1 incident. GDPR supervisory authority notified within 72 hours where personal data of EEA/UK data subjects is affected. Licensee Data Controllers notified within 24 hours. GLI notified where game integrity or RNG certification may be affected.

8. Post-Incident Review — Completed within 14 calendar days of containment. Root cause, timeline, lessons learned, and remediation actions documented and presented to the SSC.

### 14.3 IR Playbooks

Specific playbooks must be maintained and tested annually for:

- Personal data breach / unauthorised access
- Ransomware / destructive malware on AWS or endpoint
- DDoS attack — Cloudflare mitigation activation and escalation
- Insider threat / malicious privileged access
- Game integrity compromise / RNG tampering / GLI-19 breach
- Licensee API credential compromise — self-hosted vault revocation procedure
- CGA regulatory breach notification
- AWS account compromise / cloud infrastructure attack
- Critical vendor failure (AWS, Cloudflare)

### 14.4 Business Continuity & Disaster Recovery

| Parameter                             | Target                                                                                                                                                                                                              |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Recovery Time Objective (RTO)</b>  | 4 hours — game delivery API and Tier 1/Tier 2 integration endpoints; 8 hours — non-critical internal systems.                                                                                                       |
| <b>Recovery Point Objective (RPO)</b> | 1 hour — game transaction logs and financial settlement data (AWS RDS Multi-AZ + real-time replication); 4 hours — other operational data.                                                                          |
| <b>Backup Approach</b>                | Game transaction logs: real-time AWS RDS replication to a secondary region. Databases: hourly automated snapshots to S3 (cross-region). Configuration: version-controlled in the in-house repository, continuously. |
| <b>Backup Storage</b>                 | AWS S3 with cross-region replication; server-side encryption via AWS KMS. Integrity verified monthly.                                                                                                               |
| <b>DR Test Frequency</b>              | Full DR failover test annually; backup restoration tested quarterly.                                                                                                                                                |
| <b>BCP Owner</b>                      | Director (Capital Trust Corporation N.V.)/CISO                                                                                                                                                                      |

## 15. LOGGING, MONITORING & AUDIT

---

### 15.1 Mandatory Log Events

The following events must be logged across all production systems:

- All authentication events (successful, failed, MFA events, account lockouts) — Google Workspace and all systems.
- All privileged access and administrative actions — Google Cloud IAM and AWS CloudTrail.
- All changes to game configuration, RTP settings, RNG parameters, or GLI-19 certified parameters.
- All game round outcomes, settlements, and reconciliation events (including GLI-19 certificate reference per log entry).
- All licensee API authentication, authorisation, rate-limit events, and API key lifecycle events.
- All AWS CloudTrail management and data events across all accounts and regions.
- All Cloudflare WAF, DDoS, and access events (exported via Cloudflare Logpush).
- All self-hosted VPN authentication and session events.
- All secrets vault (self-hosted) access and lifecycle events.
- All AWS KMS key usage events.
- All CI/CD pipeline runs, artefact signing events, and production deployments.

### 15.2 SIEM & Centralised Monitoring

All production logs — AWS CloudTrail, Cloudflare, VPN, application logs, secrets vault, and endpoint logs — are forwarded to the Company's in-house SIEM (ELK Stack / OpenSearch, self-hosted within the AWS management VPC). Logs are retained for 12 months hot and 36 months cold in S3 Glacier. The SIEM must alert on:

- Credential stuffing or brute-force patterns — 5 or more failed logins within 5 minutes from a single source.
- Unusual API call volumes from a single licensee credential — greater than 200% of the 7-day rolling baseline.
- Access to game configuration or RNG systems in production outside an approved change window.
- Any AWS CloudTrail events involving root account usage.
- Any AWS KMS key usage events for the RNG seed CMK.
- Any self-hosted vault access events for Restricted class secrets outside of normal service account patterns.
- Bulk data access or export events from AWS S3 or RDS.
- Cloudflare security events: WAF rule triggers, DDoS alerts, or unusual origin bypass attempts.

### 15.3 Log Integrity

- Log data in S3 is stored with Object Lock (WORM mode) to prevent deletion or modification.
- AWS CloudTrail log file validation is enabled; tampering attempts generate immediate alerts.
- Time synchronisation (AWS Time Sync Service / NTP) is enforced across all instances.

- Log access is restricted to the security operations team and auditors via IAM policy.

## 15.4 Audit Rights

- CGA auditors must be granted access to game logs, RNG records, GLI-19 certificates, and technical documentation within 24 hours of a written request.
- GLI must be granted access to game build artefacts, source code (under NDA), and RNG configuration records as part of certification and re-certification activities.
- Tier 1 and Tier 2 licensees have audit rights limited to the Company's integration and data processing activities relevant to their license, on 10 business days' written notice.
- Internal security audits are conducted at minimum annually, with results reported to the SSC.

## 16. HUMAN RESOURCES & SECURITY AWARENESS

---

### 16.1 Pre-Employment Screening

- Identity verification.
- Right to work verification.
- Criminal background check (where legally permissible in the hiring jurisdiction).
- Employment history verification — minimum 3 years.
- Enhanced screening for roles with privileged AWS or vault access, financial authority, or access to Restricted data.

### 16.2 Security Awareness Training

- All employees must complete mandatory security awareness training within the first 5 working days of employment.
- Annual refresher training is mandatory for all staff; tracked by the CISO and reported to the SSC.
- Role-specific training: developers (secure coding, OWASP, GLI-19 process, AWS security); finance staff (fraud, AML); licensing/commercial staff (social engineering, phishing, licensee fraud awareness).
- Phishing simulation exercises are conducted quarterly. Staff who fail three consecutive simulations must complete targeted remedial training within 5 business days.

### 16.3 Acceptable Use Policy

All staff must adhere to the Company's Acceptable Use Policy (AUP-001), covering use of Google Workspace, AWS resources, the self-hosted VPN, Company devices, and handling of confidential information. Acknowledgement required at onboarding and annually.

### 16.4 Insider Threat

- Separation of duties and least-privilege access — enforced via Google Cloud IAM and AWS IAM — are the primary controls against insider threats.
- The whistleblowing policy provides a confidential channel for reporting suspected game manipulation, data theft, or regulatory fraud.

### 16.5 Leavers Procedure

- HR notifies IT and Security to initiate the leaver checklist upon notice of departure.
- Google Workspace account, AWS IAM access, VPN certificates, and self-hosted vault tokens are revoked on the last working day; immediately for involuntary terminations.
- Company-issued devices must be returned before final sign-off.
- Leavers are reminded of their continuing confidentiality obligations.

## 17. PHYSICAL SECURITY

---

### 17.1 Office & Facility Access

- All Company offices operate electronic access control with access logs retained for 12 months.
- Visitors must be registered and accompanied at all times within secure areas.
- CCTV is operational at entry points and in any on-premises server room areas.

### 17.2 Infrastructure Physical Security

The Company's production infrastructure is hosted on AWS. Physical security of AWS data centers is the responsibility of AWS under the shared responsibility model. AWS physical security certifications (ISO 27001, SOC 2 Type II) are reviewed annually as part of the vendor risk programme.

Any on-premises Company server infrastructure (e.g. self-hosted vault hardware) must be housed in a locked, access-controlled facility with environmental monitoring (temperature, humidity, fire suppression) and UPS backup power with a minimum 4-hour runtime.

### 17.3 Clean Desk & Clear Screen

- Employees must not leave Confidential or Restricted materials visible when away from their workstation.
- Google Workspace and other screens must lock automatically after 5 minutes of inactivity (enforced via device policy).
- Confidential or Restricted documents must be stored in locked cabinets when not in use and destroyed by cross-cut or micro-cut shredder when no longer required.

## 18. LICENSEE SECURITY REQUIREMENTS

---

### 18.1 Tier 1 (Direct Operator) Onboarding

Before receiving production API credentials (issued from the self-hosted vault), all Tier 1 licensees must:

- Pass the Company's Technical Security Onboarding Assessment (ref: OBD-T1-001).
- Confirm holding of a valid license issued by the CGA or another recognised regulatory authority.
- Sign the License Agreement incorporating the Licensee Security Schedule (LSS-001).
- Execute a Data Processing Agreement (DPA) where player data processing is involved.
- Provide IP address ranges for Cloudflare API allowlisting and confirm TLS 1.2/1.3 on all receiving endpoints.
- Acknowledge receipt of the applicable GLI-19 certificate references for all game titles being integrated.

### 18.2 Tier 2 (Reseller / Aggregator) Onboarding

In addition to Tier 1 requirements, Tier 2 licensees must:

- Provide a complete list of downstream operators, including licensing jurisdiction and regulatory authority.
- Confirm contractual mechanisms by which minimum security requirements are flowed down to downstream operators.
- Submit their downstream operator sub-license agreement (or relevant excerpts) to the Head of Legal for review before activation.
- Notify the Company within 5 business days of any change to their downstream operator network.

### 18.3 Contractual Security Obligations — All Licensees

- Maintain a valid, current license from a recognised regulatory authority for all markets where IOGr B.V.'s games are deployed.
- Deploy only game builds for which a current, valid GLI-19 certificate exists; do not modify any game build post-delivery.
- Protect API credentials (received from the Company's self-hosted vault) from unauthorised disclosure; rotate on any suspected compromise.
- Notify the Company immediately and within 4 hours upon discovering any actual or suspected compromise of integration credentials.
- Implement responsible gambling controls as required by applicable regulations; do not disable or degrade features supplied by the Company.
- Retain player game session records for a minimum of 5 years; make them available for dispute resolution upon request.
- Permit the Company to audit integration systems on 10 business days' written notice.
- Report material security incidents affecting game content or API integrity within 24 hours of discovery.

## 18.4 Shared Responsibility Matrix

| Control Domain                              | IOGr B.V.                             | Tier 1 Operator                        | Tier 2 Reseller                          |
|---------------------------------------------|---------------------------------------|----------------------------------------|------------------------------------------|
| Game logic & RNG integrity                  | Full owner (GLI-19 certified)         | Consume only                           | Consume only                             |
| Game build hash & cert verification         | Issues hash + GLI-19 cert ref         | Verify before deployment               | Verify before deployment                 |
| API credential issuance (self-hosted vault) | Full owner                            | Secure storage of own credentials      | Secure storage of own credentials        |
| Cloudflare edge protection                  | Full owner                            | None (protected at source)             | None (protected at source)               |
| Player data (PII) — Data Controller         | Not applicable                        | Full (Data Controller)                 | Full (Data Controller for their players) |
| Player KYC / AML                            | Not applicable                        | Full obligation                        | Full (own & downstream)                  |
| Responsible gambling tools                  | Technical provision                   | Activation & compliance                | Ensure downstream activation             |
| Geo-blocking                                | Cloudflare geo-restriction capability | Licensing compliance obligation        | Own & downstream compliance              |
| Downstream operator vetting                 | None                                  | None                                   | Full due diligence required              |
| Hosting & infrastructure security           | Full (AWS + Cloudflare)               | Own platform — licensee responsibility | Own platform — licensee responsibility   |

## 19. VULNERABILITY & PATCH MANAGEMENT

---

### 19.1 Vulnerability Scanning

- Automated vulnerability scans run against all internet-facing systems weekly via the in-house scanning toolset.
- Internal AWS network and instance scans run monthly using AWS Inspector and in-house tooling.
- Container images are scanned by Trivy (in-house deployment) on every CI/CD pipeline run.
- AWS Security Hub performs continuous CSPM monitoring; findings are reviewed weekly.
- All scan results are imported into the in-house vulnerability register within 24 hours of scan completion.

### 19.2 Vulnerability Register & Triage

Identified vulnerabilities are risk-scored using CVSS v3.1 or later and remediated per the SLAs in Section 13.2. The vulnerability register is reviewed weekly by the security team and monthly at the SSC.

### 19.3 Penetration Testing

- Annual external penetration test by a CREST-accredited or equivalent independent firm.
- Scope: all internet-facing game delivery infrastructure, Tier 1/Tier 2 API endpoints, licensee portal, internal AWS network (grey-box), CI/CD pipeline, and self-hosted vault.
- Critical findings: remediation within 24 hours. High findings: within 7 days. Both verified by retest.
- Reports retained for 3 years; available to the CGA or GLI within 24 hours upon request.

### 19.4 Responsible Disclosure Programme

IOGr B.V. operates a responsible disclosure programme at [security@inout.global](mailto:security@inout.global). Acknowledgement within 3 business days; remediation timeline within 7 business days. No legal action will be taken against researchers who act in accordance with the programme's terms.

## 20. COMPLIANCE & CERTIFICATION

### 20.1 CGA Regulatory Compliance

IOGr B.V. holds a license issued by the Curaçao Gaming Authority (CGA) under the National Ordinance on Offshore Games of Hazard (NOOGH). Compliance obligations include:

- All game titles and RNG systems must be certified by GLI under the GLI-19 standard before release to any licensee.
- The CGA must be notified of any material change to the technical platform, game content, or RNG implementation within the timeframe specified in the license conditions.
- Records sufficient for a CGA audit must be retained for a minimum of 5 years.
- CGA auditors must be granted access to game logs, RNG records, GLI-19 certificates, and technical documentation within 24 hours of a written request.
- Any incident constituting or potentially constituting a breach of the CGA license conditions must be reported to the CGA within 72 hours of discovery.
- All Tier 1 and Tier 2 licensees must hold a valid CGA or CGA-recognised license before receiving production access.

### 20.2 GLI-19 Certification Status

|                                 |                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------|
| <b>Testing Laboratory</b>       | Gaming Laboratories International (GLI)                                                   |
| <b>Applicable Standard</b>      | GLI-19: Standard for Online Gaming Systems (current version)                              |
| <b>Certification Scope</b>      | All game titles and RNG systems supplied by IOGr B.V.                                     |
| <b>Certificate Reference(s)</b> | MO-711-I0G-25-01-120                                                                      |
| <b>Renewal Trigger</b>          | Material change to certified game parameters; CGA technical standards cycle; CGA request. |

### 20.3 Technology Stack Compliance

|                                     |                                                                                                                                       |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>Amazon Web Services (AWS)</b>    | AWS SOC 2 Type II and ISO 27001 certifications reviewed annually. AWS shared responsibility model documented for all services in use. |
| <b>Cloudflare</b>                   | Cloudflare SOC 2 Type II certification reviewed annually. DDoS SLA and WAF configuration reviewed quarterly.                          |
| <b>AWS KMS</b>                      | AWS KMS is FIPS 140-2 validated. Key policies and usage logs reviewed quarterly.                                                      |
| <b>Self-Hosted Secrets Vault</b>    | HashiCorp Vault deployment audited annually. Vault HA configuration and unseal procedures tested semi-annually.                       |
| <b>Self-Hosted VPN</b>              | VPN configuration reviewed quarterly against security baseline. VPN software maintained at current patched version.                   |
| <b>Google Workspace / Cloud IAM</b> | Google Workspace security centre reviewed quarterly. IAM role assignments reviewed and recertified quarterly.                         |

## 20.4 Annual Policy Review

This Policy is reviewed annually by the CISO. Reviews consider: changes in the threat landscape; CGA or GLI-19 standard updates; GDPR or AML regulatory developments; lessons learned from incidents; penetration test and audit results; and changes to the Company's AWS infrastructure, technology stack, or business model. All material changes require sign-off from the Director (Capital Trust Corporation N.V.) and CISO before reissue.

## APPENDIX A — KEY CONTACTS

| Role                                 | Name                           | Contact                                                                      |
|--------------------------------------|--------------------------------|------------------------------------------------------------------------------|
| Director / Authorised Representative | Capital Trust Corporation N.V. | kyc@inout.global                                                             |
| CISO                                 | Jason Lee Jr.                  | jason.lee.jr@inout.global                                                    |
| DPO                                  | Zachary Taylor                 | zachary.tl@inout.global                                                      |
| MLRO                                 | Oliver Thomas                  | park.alisha@inout.global                                                     |
| Head of Legal & Compliance           | Alisha Park                    | legal@inout.global                                                           |
| GLI Liaison                          | Alberto Ruiz-Ocana             | <a href="mailto:a.ruiz-ocana@gaminglabs.com">a.ruiz-ocana@gaminglabs.com</a> |

## APPENDIX B — RELATED DOCUMENTS

|                                                |                    |
|------------------------------------------------|--------------------|
| AML & CTF Policy                               | AML-001            |
| Acceptable Use Policy                          | AUP-001            |
| Data Retention Policy                          | DRP-001            |
| Business Continuity Plan                       | BCP-001            |
| Incident Response Playbooks                    | IRP-001 to IRP-009 |
| Secure Coding Guidelines                       | SCG-001            |
| Licensee Security Schedule (contract exhibit)  | LSS-001            |
| Tier 1 Technical Security Onboarding Checklist | OBD-T1-001         |
| Tier 2 Reseller Onboarding Checklist           | OBD-T2-001         |
| Change Management Procedure                    | CMP-001            |
| AWS Security Baseline & CIS Benchmark Mapping  | AWS-SEC-001        |
| Cloudflare WAF Ruleset Documentation           | NET-SEC-001        |
| Self-Hosted Vault Operations Runbook           | VAULT-OPS-001      |
| Whistleblowing Policy                          | HR-003             |

|                                                           |          |
|-----------------------------------------------------------|----------|
| <b>HR Disciplinary Policy</b>                             | HR-001   |
| <b>Record of Processing Activities (RoPA)</b>             | DPO-001  |
| <b>Compliance Mapping Matrix (CGA, GLI-19 &amp; GDPR)</b> | COMP-001 |

## APPENDIX C — DEFINITIONS

|                   |                                                                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AML / CTF</b>  | Anti-Money Laundering / Counter-Terrorism Financing.                                                                                                   |
| <b>API</b>        | Application Programming Interface.                                                                                                                     |
| <b>AWS</b>        | Amazon Web Services — the Company's cloud infrastructure provider.                                                                                     |
| <b>AWS KMS</b>    | AWS Key Management Service — the Company's primary key management system for all encryption keys.                                                      |
| <b>B2B</b>        | Business-to-Business. All IOGr B.V. commercial relationships are B2B; the Company does not operate consumer-facing gambling products.                  |
| <b>BCP / DR</b>   | Business Continuity Plan / Disaster Recovery.                                                                                                          |
| <b>CGA</b>        | Curaçao Gaming Authority — the primary licensing and regulatory authority for IOGr B.V.                                                                |
| <b>CISO</b>       | Chief Information Security Officer.                                                                                                                    |
| <b>Cloudflare</b> | The Company's DDoS mitigation, WAF, and CDN edge provider.                                                                                             |
| <b>CSPM</b>       | Cloud Security Posture Management. Implemented via AWS Security Hub.                                                                                   |
| <b>CVSS</b>       | Common Vulnerability Scoring System (v3.1 or later).                                                                                                   |
| <b>Director</b>   | Capital Trust Corporation N.V., the duly appointed Director of IOGr B.V.                                                                               |
| <b>DPA</b>        | Data Processing Agreement.                                                                                                                             |
| <b>DPO</b>        | Data Protection Officer.                                                                                                                               |
| <b>GDPR</b>       | General Data Protection Regulation (EU) 2016/679 and / or UK GDPR as applicable.                                                                       |
| <b>GLI</b>        | Gaming Laboratories International — the independent testing laboratory for all IOGr B.V. GLI-19 certifications.                                        |
| <b>GLI-19</b>     | The Gaming Laboratories International Standard for Online Gaming Systems. All IOGr B.V. game titles and RNG systems are certified under this standard. |

|                                     |                                                                                                          |
|-------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Google Workspace / Cloud IAM</b> | The Company's identity, email, collaboration, and PAM platform.                                          |
| <b>ISMS</b>                         | Information Security Management System.                                                                  |
| <b>JIT</b>                          | Just-in-Time privileged access (implemented via Google Cloud IAM Conditions and AWS IAM session tokens). |
| <b>MLRO</b>                         | Money Laundering Reporting Officer.                                                                      |
| <b>NOOGH</b>                        | National Ordinance on Offshore Games of Hazard (Curaçao) — the legislative basis for CGA licensing.      |
| <b>RNG</b>                          | Random Number Generator.                                                                                 |
| <b>RoPA</b>                         | Record of Processing Activities.                                                                         |
| <b>RPO</b>                          | Recovery Point Objective.                                                                                |
| <b>RTO</b>                          | Recovery Time Objective.                                                                                 |
| <b>SAR</b>                          | Suspicious Activity Report.                                                                              |
| <b>SBOM</b>                         | Software Bill of Materials.                                                                              |
| <b>Self-Hosted Vault</b>            | The Company's self-hosted HashiCorp Vault deployment used for secrets management.                        |
| <b>Self-Hosted VPN</b>              | The Company's self-hosted VPN solution (WireGuard / OpenVPN) for remote access.                          |
| <b>SIEM</b>                         | Security Information and Event Management — the Company's in-house ELK Stack / OpenSearch deployment.    |
| <b>SSC</b>                          | Security Steering Committee.                                                                             |
| <b>Tier 1 Licensee</b>              | A direct operator that publishes IOGr B.V.'s games on a consumer-facing platform.                        |
| <b>Tier 2 Licensee</b>              | A reseller or aggregator that sub-licences IOGr B.V.'s games to downstream operators.                    |
| <b>TLS</b>                          | Transport Layer Security.                                                                                |

## APPENDIX D — EXCEPTION MANAGEMENT

Any deviation from this Policy requires a formal written exception request submitted to the CISO. The CISO may approve exceptions where a documented risk-based justification exists and appropriate compensating controls are in place. Exceptions to CGA-mandated controls or GLI-19 certification requirements must be escalated to the Director (Capital Trust Corporation N.V.) for approval.

All approved exceptions must:

- Be documented with a unique reference number, named owner, compensating controls, risk acceptance rationale, and a maximum 6-month expiry date.
- Be reviewed by the CISO every 6 months; exceptions not renewed lapse automatically.
- Be reported at the next SSC meeting following approval.
- Be escalated to the Director for approval where they relate to a CGA-mandated or GLI-19 certification control.

Exception requests must be submitted to: Jason.lee.jr@inout.global with the subject line 'ISP Exception Request'.

---

— End of Document · IOGr B.V. Information Security Policy · Version 1.0 —