

INFORMATION SECURITY CONTROL POLICY

(B2B Game Development Organization)

1. Purpose

Chancers Technology B.V. ("the Company") is committed to maintaining a robust Information Security Management System (ISMS) to protect its information assets, support secure business operations, and manage information security risks effectively.

This Information Security Control Policy defines the framework for managing information security risks within the organization. It ensures the confidentiality, integrity, and availability of company systems, software products, and development environments.

The policy is aligned with applicable requirements of the Curaçao Gaming Authority (CGA) and supports the secure development and delivery of gaming software to licensed operators/ customers.

2. Scope

This policy applies to all employees, contractors, consultants, and third parties involved in the development, maintenance, testing, and support of the organization's systems and software.

The organization operates **strictly** as a **business-to-business (B2B) game developer** and:

- Does not interact directly with end users or players
- Does not collect, process, or store player personal data
- Does not operate gaming platforms or manage player accounts

Scope includes:

- Development environments (dev/test/staging)
- Source code repositories and CI/CD pipelines
- Internal IT infrastructure and cloud services
- Business and technical operational data

3. Information Security Governance

- Information Security Officer (ISO) is responsible for operational oversight.
- Senior (Operational) Management ensures implementation.
- Compliance with CGA Information Security Control Requirements is mandatory

- All staff must comply with this policy.
- The Board of Directors retains ultimate oversight and accountability for information security governance.

4. Risk Management

- Risk-based approach applied across systems.
- Annual and change-based risk assessments required.
- Risks must be documented, assessed, and treated or accepted by management.

5. Access Control

- Least privilege enforced.
- Unique user accounts required.
- Shared accounts prohibited unless approved.
- MFA required for privileged access.
- Quarterly access reviews mandatory.
- Immediate revocation upon termination or role change.

6. Secure Software Development Lifecycle (SDLC)

- Security integrated throughout SDLC.
- Secure coding standards enforced.
- Mandatory code review prior to deployment.
- Regular vulnerability scanning and testing.
- Controlled release and change management.

7. Change Management

- All changes must be approved, documented, and risk-assessed.
- Emergency changes require post-review validation.
- Segregation of duties enforced.

8. Incident Management (Enhanced)

8.1 Definition of Incident (CGA Context)

An incident is defined in accordance with the Curaçao Gaming Authority (CGA) framework under the Landsverordening op de Kansspelen (LOK), Article 5.10.

An incident is any event that may affect the integrity, security, fairness, availability, or proper functioning of a licensed gambling operation.

For the purposes of this policy, incidents are interpreted broadly and include technical, operational, or compliance-related events that could materially impact a Customer / Software Licensee's regulated gaming environment.

8.2 Incident Types Relevant to a Game Developer

Although the organization does not operate gaming platforms or process player data, the following categories are considered reportable or relevant incidents due to their potential impact on licensed operations:

A. Software / Product Integrity Incidents

- Defects in game logic affecting randomness, RTP, or game outcomes
- Incorrect payout calculations or bonus logic errors
- Version release errors impacting production builds
- Corrupted or incomplete game builds deployed to production environments
- Critical bugs affecting game availability or stability

B. Security Incidents (Developer Environment)

- Unauthorized access to source code repositories
- Compromise of CI/CD pipelines or build systems
- Leakage of proprietary game logic or algorithms
- Malware or ransomware affecting development infrastructure
- Misuse of credentials or privileged accounts

C. Infrastructure / Availability Incidents

- Cloud or hosting outages affecting deployed game services
- CI/CD pipeline failure blocking deployments
- DNS, API, or integration failures impacting game functionality
- Loss of connectivity between development and production environments

D. Release / Deployment Incidents

- Incorrect deployment to production environments
- Failure to follow approved change management procedures
- Hotfixes introduced without proper validation
- Rollback failures or inability to restore stable version

E. Compliance / Operational Risk Incidents

- Deviations from approved technical specifications required by Customer / Software Licensee
- Failure of required security controls in delivered software
- Any condition that may compromise CGA compliance obligations of the Customer / Software Licensee
- Material defects that could impact regulatory reporting or auditability

8.3 Incident Detection and Identification

Incidents may be identified through:

- Automated monitoring and logging systems
- Internal QA or testing processes
- Developer or DevOps observation
- Customer / Software Licensee notification
- Security tools (e.g., vulnerability scanners, SIEM alerts)

All personnel are required to report suspected incidents immediately upon discovery.

8.4 Incident Reporting Process

Step 1 – Immediate Internal Reporting

- The individual identifying the incident must immediately notify:
 - IT/DevOps team
 - Information Security Officer (ISO)
 - Relevant system owner
- Initial notification must occur without delay and within the same business day where possible.

Step 2 – Initial Classification

The ISO or designated incident lead shall:

- Classify severity (Critical / High / Medium / Low)
- Determine whether the incident may impact:
 - Production systems
 - Customer / Software Licensee operations
 - Regulatory obligations
- Determine whether CGA reporting is potentially required under Article 5.10.

Step 3 – Containment and Mitigation

- Immediate steps must be taken to contain the issue
- Actions may include rollback, disabling features, isolating systems, or revoking access
- Priority is given to preventing further impact on licensed operations

Step 4 – Internal Escalation

- Critical or high severity incidents must be escalated to Senior Management immediately
- A dedicated incident log must be opened documenting:
 - Timeline of events
 - Systems affected
 - Initial impact assessment
 - Containment actions

Step 5 – CGA Reporting Assessment

The ISO, in consultation with Senior Management, must determine whether the incident is reportable under Article 5.10 LOK, based on whether it:

- Impacts integrity, availability, or security of gaming operations
- Affects systems supporting regulated gambling services
- May impact Customer / Software Licensee compliance obligations
- Falls within CGA-defined categories of operational incidents

Step 6 – CGA Submission (Where Applicable)

Where reportable, the incident must be submitted to the CGA:

- Without undue delay, and
- No later than 24 hours after detection, in accordance with Article 5.10(6)
- Incident report template will be completed and filed with the Board of Directors, particularly the Local Management in Curacao

Submission must include:

- Incident description
- Time of detection and timeline
- Systems affected
- Root cause (if known at time of submission)
- Mitigation actions taken
- Current status (open/contained/resolved)

Step 7 – Follow-up Reporting

- A final incident report must be prepared once resolved
- Must include:
 - Root cause analysis (RCA)
 - Corrective and preventive actions (CAPA)
 - Lessons learned
- Shared with Customer / Software Licensee where relevant
- Filed with the Local Management in Curacao

8.5 Communication Protocol

- Internal communication must be controlled by the ISO or appointed incident lead
- Unauthorized communication about incidents is prohibited
- Customer / Software Licensee must be informed when production or regulatory impact exists
- Communication must be factual, time-stamped, and consistent

8.6 Record Keeping

- All incidents must be logged in a central incident register
- Records must be retained for audit and regulatory purposes
- Logs must include evidence of decision-making for CGA reporting decisions

9. Logging and Monitoring

- Security logs must be generated and protected.
- Logs must be tamper-resistant.
- Monitoring required for anomalies and threats.
- Logs must support auditability.

10. Infrastructure Security

- Segregation of environments required.
- Secure network configuration enforced.
- Cloud environments must follow best practices.
- Periodic configuration reviews required.

11. Third-Party Management

- Security due diligence required.
- Contracts must include confidentiality clauses.
- Access must be controlled and monitored.
- Access revoked upon termination.

12. Data Protection

- No player or end-user data is processed or stored.
- Only internal operational and development data is handled.
- Data must be protected against unauthorized access or disclosure.
- Test data must be anonymized or synthetic where possible.
- Encryption required for sensitive data in transit and at rest.

12A. Intellectual Property Protection

The organization recognizes its intellectual property as a critical business asset and shall implement appropriate measures to protect proprietary information from unauthorized access, disclosure, modification, reproduction, or distribution.

Intellectual property includes, but is not limited to:

- Source code and software applications
- Game mechanics, game logic, and mathematical models
- Random Number Generator (RNG) implementations
- Game artwork, graphics, animations, audio, and visual assets
- Software architecture and technical documentation
- Product roadmaps, specifications, and development methodologies
- Trade secrets, proprietary algorithms, and business information

To protect intellectual property, the organization shall:

- Restrict access to intellectual property assets on a need-to-know basis and in accordance with the principle of least privilege.
- Maintain appropriate access controls for source code repositories, development environments, and document management systems.
- Require all employees, contractors, and third-party service providers to be bound by confidentiality and non-disclosure obligations.
- Implement version control systems and audit trails to track changes to software and related assets.
- Protect intellectual property through appropriate technical safeguards, including encryption, secure storage, monitoring, and backup procedures.
- Prohibit the unauthorized copying, transmission, disclosure, or use of proprietary information.
- Ensure intellectual property remains the exclusive property of the organization unless otherwise contractually agreed with a Customer / Software Licensee.
- Investigate and address any suspected loss, theft, misuse, or unauthorized disclosure of intellectual property as an information security incident.

Where intellectual property is shared with a Customer / Software Licensee, supplier, certification laboratory, or regulatory authority, such disclosure shall be limited to the minimum necessary information and protected through appropriate contractual, legal, and technical safeguards.

13. Business Continuity & Disaster Recovery

13.1 RTO & RPO

- **RTO (Recovery Time Objective):** Critical systems must be restored within 4–24 hours depending on severity classification.
- **RPO (Recovery Point Objective):** Data loss must be minimized; critical systems aim for near-zero data loss where feasible.

13.2 Backups

- Offsite encrypted backups required.
- Geographically separated storage must be used.
- Daily backups for critical systems.
- Backup restoration testing required.

13.3 Scenarios Covered

- Cybersecurity incidents
- Infrastructure or cloud outages
- Deployment failures
- Hardware or storage failure
- Environmental or disaster events

13.4 Roles & Responsibilities

- Management: Approval and oversight
- IT/DevOps: Execution of recovery and backups
- ISO: Oversight and coordination
- System Owners: Validation of restored services

13.5 Communication

- Immediate escalation to management required.

- Internal updates during disruption.
- Notification to Customer / Software Licensee where production systems are impacted.

14. Compliance and Audit

- Compliance with applicable CGA requirements is mandatory.
- Internal audits may be conducted.
- Non-compliance may result in disciplinary or contractual action.

15. Customer / Software Licensee Responsibility

- The Customer / Software Licensee is responsible for obtaining and maintaining all regulatory approvals, licenses, certifications, and authorizations applicable to its licensed activities.
- This includes all gaming operations and player-facing compliance obligations arising under its license and applicable regulatory requirements.
- Organization provides technical support where required.
- Regulatory accountability remains with Customer / Software Licensee.

16. Policy Review

Annual review or upon significant change.

CGA COMPLIANCE MAPPING & GAP ANALYSIS

CGA Control Domain	Requirement Area	Policy Section	Coverage Status	Key Controls / Evidence
Governance & Oversight	Board accountability and security governance	§3 Information Security Governance	Fully Covered	Board retains ultimate oversight; ISO assigned operational responsibility
Risk Management	Formal risk-based security approach	§4 Risk Management	Fully Covered	Annual + change-triggered risk assessments; documented risk treatment
Access Control	Least privilege, authentication, access governance	§5 Access Control	Fully Covered	Unique accounts, MFA, quarterly access reviews, revocation process

CGA Control Domain	Requirement Area	Policy Section	Coverage Status	Key Controls / Evidence
Secure Development (SDLC)	Secure coding, testing, release controls	§6 SDLC	Fully Covered	Secure coding standards, code review, vulnerability testing, controlled deployments
CGA Control Domain	Requirement Area	Policy Section	Coverage Status	Key Controls / Evidence
Information Asset Protection	Protection of proprietary information, source code, and development assets	§12A Intellectual Property Protection	Fully Covered	Access controls, NDAs, repository security, encryption, audit trails, incident handling
Change Management	Controlled system changes and approvals	§7 Change Management	Fully Covered	Approved changes, emergency change review, segregation of duties
Incident Management (LOK Art. 5.10)	Incident definition, classification, reporting	§8 Incident Management	Fully Covered	Legal definition integrated, broad interpretation applied
Incident Reporting SLA	24-hour reporting requirement to CGA	§8.2 Incident Management	Fully Covered	Explicit “within 24 hours of detection” requirement included
Logging & Monitoring	Audit logs and security monitoring	§9 Logging & Monitoring	Fully Covered	Tamper-resistant logs, anomaly detection, audit readiness
Infrastructure Security	System and network protection controls	§10 Infrastructure Security	Fully Covered	Environment segregation, secure cloud configuration
Third-Party Risk Management	Vendor security and access control	§11 Third-Party Management	Fully Covered	Due diligence, contractual controls, access restrictions
Data Protection	Confidentiality, secure handling of data	§12 Data Protection	Fully Covered	No player data, encryption,

CGA Control Domain	Requirement Area	Policy Section	Coverage Status	Key Controls / Evidence
				anonymization, secure storage
Business Continuity (BCP)	Service continuity and resilience planning	§13 Business Continuity & DR	Fully Covered	Defined RTO/RPO, disaster scenarios, recovery planning
Disaster Recovery (DR)	Backup, restoration, offsite resilience	§13 Business Continuity & DR	Fully Covered	Offsite encrypted backups, restore testing, redundancy
Communication & Escalation	Incident/disruption communication flows	§13 Business Continuity & DR	Fully Covered	Internal escalation + licensee notification framework
Regulatory Responsibility Split	Operator vs developer obligations	§15 Customer / Software Licensee Responsibility	Fully Covered	Clear allocation of regulatory accountability
Compliance & Audit	Internal audit and regulatory compliance	§14 Compliance and Audit	Fully Covered	Auditability and compliance monitoring included
Policy Governance	Policy maintenance and review cycle	§16 Policy Review	Fully Covered	Annual review requirement established

By: _____



Name: Pablo Najar Rojas

Title: Chief Technology Officer