



Information Security Policy

Comprehensive data protection and cybersecurity framework aligned with CGA technical standards and industry best practices.

v1.0

☐ Draft

TABLE OF CONTENTS

1.0

Purpose & Scope

This Information Security Policy establishes the framework for protecting the confidentiality, integrity, and availability of all information assets, systems, and data processed by the operator. It applies to all employees, contractors, third-party vendors, and any individual with access to the operator's information systems.

The policy covers all aspects of information security including physical, technical, and administrative controls for the gaming platform, internal systems, player data, financial records, and corporate information.

2.0

Information Security Governance

Chief Technology Officer (CTO) / Chief Information Security Officer (CISO): Responsible for the overall information security program, including policy development, risk management, and security operations.

Board Oversight: The Board receives quarterly information security reports covering threat landscape, incident summaries, risk status, and compliance posture.

Security Committee: A cross-functional committee meets monthly to review security matters, approve changes, and coordinate security initiatives. Members include CTO/CISO, Compliance Officer, Head of Operations, and external security advisors (as required).

3.0

Risk Management

The operator conducts regular information security risk assessments:

- **Annual Comprehensive Risk Assessment:** Full evaluation of threats, vulnerabilities, and controls across

all systems

- **Change-Triggered Assessments:** Conducted when significant changes are made to infrastructure, applications, or processes
- **Threat Intelligence:** Continuous monitoring of emerging threats specific to the online gaming industry
- **Risk Register:** Maintained and updated with identified risks, assessed impact/likelihood, and mitigation controls

4.0 Access Control

Principle of Least Privilege: All access is granted on a need-to-know, need-to-use basis.

- **Authentication:** Multi-factor authentication (MFA) mandatory for all administrative access, VPN connections, and critical systems
- **Password Policy:** Minimum 12 characters, complexity requirements, 90-day rotation for privileged accounts, no password reuse (last 12)
- **Access Reviews:** Quarterly access reviews for all systems; immediate revocation upon role change or termination
- **Privileged Access Management (PAM):** Dedicated privileged access management system with session recording, just-in-time access, and audit logging
- **Player Account Security:** Optional MFA for player accounts, account lockout after 5 failed attempts, password reset procedures

5.0 Network & Infrastructure Security

- **Firewalls & Segmentation:** Network segmented into security zones; firewalls control traffic between zones. Gaming platform, payment processing, and administrative systems are on separate network segments.
- **DDoS Protection:** Enterprise-grade DDoS mitigation services with automatic detection and response
- **Intrusion Detection/Prevention (IDS/IPS):** Network and host-based intrusion detection with real-time alerting
- **Web Application Firewall (WAF):** Protecting the gaming platform from OWASP Top 10 vulnerabilities
- **VPN:** All remote administrative access via encrypted VPN connections
- **Patch Management:** Critical patches applied within 48 hours; all others within 30 days. Automated vulnerability scanning weekly.

6.0 Data Protection & Encryption

- **Encryption in Transit:** TLS 1.2+ for all communications; HSTS enforced; certificate management and rotation
- **Encryption at Rest:** AES-256 encryption for all stored player data, financial records, and sensitive information
- **Key Management:** Hardware Security Modules (HSM) or equivalent for cryptographic key management; key rotation procedures documented
- **Data Classification:** All data classified as Public, Internal, Confidential, or Restricted with appropriate handling procedures for each level
- **PCI DSS Compliance:** Payment card data handled in compliance with PCI DSS requirements; SAQ or ROC as applicable
- **Data Retention & Destruction:** Data retained per regulatory requirements (minimum 5 years for KYC/AML records); secure destruction procedures for expired data

7.0 Application Security

- **Secure Development Lifecycle (SDL):** Security requirements defined at design phase; code reviews, static analysis (SAST), and dynamic testing (DAST)
- **Penetration Testing:** Annual external penetration testing by accredited third parties; retesting after remediation of critical findings
- **Vulnerability Management:** Continuous vulnerability scanning; prioritized remediation based on CVSS scores and business impact
- **API Security:** Authentication, rate limiting, input validation, and monitoring for all APIs
- **RNG Certification:** All Random Number Generators independently certified by accredited testing laboratories

8.0 Incident Response

Incident Response Plan (IRP): Documented, tested, and regularly updated plan covering:

- **Detection & Analysis:** 24/7 security monitoring with defined escalation procedures. SIEM platform aggregating logs from all critical systems.
- **Classification:** Incidents classified by severity (Critical, High, Medium, Low) with defined response times
- **Containment:** Immediate actions to limit impact; isolation of affected systems
- **Eradication & Recovery:** Root cause analysis; system restoration from verified clean backups

- **Post-Incident Review:** Lessons learned documented; controls updated to prevent recurrence
- **Regulatory Notification:** CGA notified of significant security incidents within 24 hours as required. Player notification where personal data is affected.

9.0 Business Continuity & Disaster Recovery

- **Business Continuity Plan (BCP):** Documented plan for maintaining critical operations during disruptions
- **Disaster Recovery Plan (DRP):** Recovery procedures for all critical systems with defined RTO (Recovery Time Objective) and RPO (Recovery Point Objective)
- **Backup Strategy:** Automated daily backups; encrypted; stored at geographically separate locations; regular restoration testing
- **Redundancy:** Active-passive or active-active failover for critical systems; geographically distributed infrastructure
- **Testing:** BCP/DRP tested at least annually through tabletop exercises and technical drills

10.0 Third-Party Security

All third-party vendors with access to operator systems or player data must:

- Undergo security due diligence assessment before engagement
- Sign data processing agreements with defined security obligations
- Provide evidence of security certifications (ISO 27001, SOC 2, PCI DSS as applicable)
- Submit to periodic security reviews and audits
- Comply with the operator's information security policies

11.0 Security Awareness Training

- Mandatory security awareness training at onboarding
- Annual refresher training for all staff
- Phishing simulations conducted quarterly
- Specialized training for development, operations, and security teams
- Security bulletins distributed for emerging threats

12.0 Compliance & Audit

- **Internal Audits:** Quarterly internal security audits assessing control effectiveness
- **External Audits:** Annual external security audit by accredited firm
- **CGA Reporting:** Security posture reports submitted to CGA as required
- **Certifications:** Pursuit of ISO 27001 certification and SOC 2 Type II report

13.0 Policy Review

This Information Security Policy is reviewed at least annually, or following significant security incidents, technology changes, or regulatory updates. All amendments are approved by the CTO/CISO and Board of Directors, and communicated to all staff.