

IT Security Protocol (for CGA licensed casino)

Document Title	IT Security Protocol for Games & More BV
Document Classification	Internal - Confidential
Document Version	1.2
Document Date	01/10/2025
Approved by	Raymond Saliba - CTO Next Review: 30/08/2026

Table of Contents

1. Purpose	3
2. Scope	3
3. Definitions and Roles.....	4
4. Risk Assessment and Asset Inventory	6
5. Access Control and Identity Management	8
6. Network and Infrastructure Security	11
7. Application and Game Engine Security.....	14
8. Data Protection and Encryption	17
9. Business Continuity and Disaster Recovery (BC/DR)	20
10. Incident Response and Reporting	23
11. Vendor and Third-Party Management	26
12. Monitoring, Logging and Audit.....	29
13. Policy and Awareness Training	31
14. Compliance and Review.....	33
Appendix A – Abbreviations and Definitions.....	35
Appendix B – Reference Documents	37
Appendix C – Document Control	37
Appendix D – Policy Acknowledgement Form	38

1. Purpose

This protocol establishes the technical and operational security controls that Games & More BV must implement to ensure the **confidentiality, integrity, and availability** of its systems, data (including player information), and services in full compliance with the regulatory requirements of the **Curaçao Gaming Authority (CGA)** and applicable laws, including the **National Ordinance for Games of Chance**, **AML/CFT** legislation, and **data-protection regulations**.

It also aligns with international best-practice frameworks such as **ISO 27001**, **ISO 27002**, and **ISO 22301**, supporting the company's overarching objective to maintain a secure, resilient, and compliant gaming environment.

2. Scope

This protocol applies to all information assets, systems, and activities within Games & More BV's operational and technical environment.

It encompasses all infrastructure and services — including networks, servers, databases, applications, payment systems, crypto infrastructure, game engines, and both on-premises and cloud-hosted platforms.

The policy's protocol applies to all personnel who access or manage these systems, including employees, contractors, consultants, vendors, and third-party service providers acting on behalf of Games & More BV.

It also extends to data and operations managed remotely or through partner integrations to ensure consistent protection across the entire gaming ecosystem.

The scope ensures that all information-security controls are applied uniformly across the organization, supporting compliance with Curaçao Gaming Authority requirements and international security standards.

3. Definitions and Roles

To ensure effective governance and accountability, Games & More BV defines the following key information-security roles and responsibilities.

Each role contributes to enforcing this IT Security Protocol and maintaining compliance with the Curaçao Gaming Authority (CGA) and applicable laws.

1. Chief Technology Officer (CTO) –

- a. Holds overall responsibility for the implementation, governance, and continuous improvement of the company's information-security program.
- b. Approves all IT-security policies, allocates resources, and ensures alignment with business and regulatory objectives.

2. Security Manager –

- a. Oversees the day-to-day management of technical and operational security controls.
- b. Coordinates vulnerability management, monitoring, and incident-response activities.
- c. Reports security status, threats, and control effectiveness to the CTO and Compliance Officer.

3. Compliance Officer –

- a. Ensures adherence to Curaçao regulatory obligations, AML/CFT laws, and data-protection requirements.
- b. Monitors policy/protocol compliance, manages regulatory submissions, and oversees reporting of incidents to the CGA or other authorities.
- c. Maintains audit evidence and coordinates external audits.

4. System Owner / Application Owner –

- a. Responsible for the security, maintenance, and compliance of specific systems or applications under their control.
- b. Ensures appropriate access control, patching, and data-handling practices within their domain.

5. User / Administrator –

- a. Operates company systems in line with approved privileges and responsibilities.

- b. Must follow all information-security policies, training requirements, and reporting obligations.
- c. Administrators are responsible for ensuring that configurations and changes comply with approved procedures.

6. Vendor / Third-Party –

- a. Refers to any external service provider with access to company systems, data, or facilities.
- b. Must comply with contractual security requirements and maintain equivalent levels of data protection and incident-reporting capability (see Section 11 – Vendor and Third-Party Management).

These defined roles establish clear accountability for maintaining information security, ensuring that Games & More BV operates with transparency, compliance, and effective oversight in alignment with Curaçao Gaming Authority requirements.

4. Risk Assessment and Asset Inventory

Games & More BV maintains a structured approach to identifying, classifying, and managing information assets and associated risks.

This framework ensures that security controls remain proportionate to asset value, business impact, and regulatory obligations under the Curaçao Gaming Authority (CGA) and international information-security standards.

1. Asset Inventory Management –

- a. An up-to-date inventory of all information assets must be maintained, including hardware, software, network devices, data repositories, and cloud resources.
- b. Each asset record must include owner, location, purpose, configuration details, and classification level.
- c. The inventory must be reviewed and verified at least **annually** or following significant infrastructure or business changes.

2. Asset Classification and Ownership –

- a. All assets must be classified according to sensitivity and criticality using defined categories such as **Public**, **Internal**, **Confidential**, and **Strictly Confidential**.
- b. Every asset must have a designated **owner** responsible for ensuring appropriate protection, usage, and lifecycle management.
- c. Access permissions, retention periods, and handling procedures must align with each asset's classification.

3. Risk Assessment –

- a. Comprehensive information-security risk assessments must be conducted at least **annually**, and whenever material changes occur (e.g., new systems, regulatory updates, mergers, or technology shifts).
- b. The assessment must evaluate threats, vulnerabilities, likelihood, and potential business impact across confidentiality, integrity, and availability dimensions.

- c. Risk findings must be documented in a centralized ***Risk Register*** maintained by the Compliance Officer and Security Manager.

4. Risk Treatment and Mitigation –

- a. Identified risks must be addressed through an approved ***Risk Treatment Plan***, outlining mitigation actions, control ownership, and completion timelines.
- b. Residual risk levels must be accepted formally by senior management where complete mitigation is impractical.
- c. Progress on mitigation actions must be tracked and reviewed at least quarterly.

5. Continuous Improvement –

- a. Results of risk assessments and mitigation reviews must inform updates to security policies, procedures, and awareness training.
- b. Lessons learned from incidents and audits must be integrated into the next assessment cycle.

These processes ensure that Games & More BV maintains an accurate view of its assets, proactively manages risks, and aligns all security controls with Curaçao Gaming Authority and international information-security standards.

5. Access Control and Identity Management

Games & More BV enforces strict identity and access-management (IAM) controls to ensure that only authorized individuals can access systems, data, and applications in accordance with the principles of least privilege, accountability, and regulatory compliance.

1. Access Control Principles –

- a. Access rights must be granted strictly according to the **principle of least privilege**, ensuring users receive only the minimum permissions required to perform their assigned duties.
- b. Access must be based on defined job roles, and all privileged access must be limited, logged, and subject to periodic review.

2. Authentication and Authorization –

- a. All administrative and remote-access accounts must be protected with **multi-factor authentication (MFA)**.
- b. Strong authentication must be used for all critical systems, with centralized identity management wherever feasible (e.g., Active Directory, SSO, or identity provider with audit capability).
- c. Shared or generic accounts are strictly prohibited unless explicitly approved by management for operational necessity and controlled via strong logging and monitoring.

3. Password and Credential Policy –

- a. Passwords must meet minimum complexity requirements: **at least 12 characters, including uppercase, lowercase, numeric, and special characters**.
- b. Games & More BV enforces **event-based password rotation** (e.g., after suspected compromise, privilege elevation, or system migration) rather than routine calendar-based expiry.
- c. Passwords must be **screened** against known-breached password lists and organizational blocklists.

- d. **Default credentials must be changed** prior to deployment.
- e. All credentials, API keys, and cryptographic secrets must be stored securely in an **encrypted secrets-management system**.
- f. Multi-Factor Authentication (**MFA**) **remains mandatory** for all administrative and remote-access accounts.

4. **Account Provisioning and De-Provisioning –**

- a. User account creation and modification must follow a formal approval workflow managed jointly by HR and IT.
- b. Departing or role-changing employees must have access revoked immediately upon termination or transfer.
- c. Service and system accounts must be reviewed and approved by the Security Manager and maintained in an inventory.
- d. Access reviews must be conducted at least **quarterly**, with results documented and approved by the Compliance Officer.

5. **Segregation of Duties –**

- a. No single individual may hold conflicting roles or responsibilities that could lead to unauthorized or unreviewed actions (e.g., development and production access, change approval and implementation, transaction initiation and approval).
- b. Critical tasks must require dual authorization where applicable.

6. **Privileged Access Management (PAM) –**

- a. Administrative access must be managed through a **Privileged Access Management (PAM)** system or equivalent controls, ensuring session logging, password rotation, and just-in-time access.
- b. All administrative actions must be logged and reviewed regularly.

7. **Third-Party and Vendor Access –**

- a. Vendors or third parties requiring system access must use dedicated, time-limited accounts with MFA enabled.

- b. Access must be monitored, logged, and revoked immediately upon completion of their tasks or contract.
- c. Vendor-access records must be reviewed periodically by the Security Manager.

8. Access Monitoring and Audit –

- a. Access events, including logins, permission changes, and privilege escalations, must be logged and forwarded to the centralized monitoring platform (see Section 12 – Monitoring, Logging and Audit).
- b. Any anomalies or unauthorized access attempts must be investigated promptly and escalated under the incident-response process (see Section 10 – Incident Response and Reporting).

These access-control measures ensure that Games & More BV maintains a secure and accountable identity-management environment in compliance with Curaçao Gaming Authority and international information-security standards.

6. Network and Infrastructure Security

Games & More BV maintains multiple layers of technical and operational controls to protect the confidentiality, integrity, and availability of its network, systems, and hosted environments.

This framework ensures resilient, segmented, and continuously monitored infrastructure that aligns with Curaçao Gaming Authority (CGA) requirements and recognized international security standards.

1. Network Segmentation and Architecture –

- a. The corporate network must be logically segmented into zones such as **production, development, staging, testing, vendor, and guest** environments.
- b. Only authorized and necessary network paths may exist between segments, enforced by firewalls and access-control lists.
- c. Systems handling player or financial data must reside only within protected production segments.

2. Perimeter Security –

- a. Firewalls and **Intrusion Detection/Prevention Systems (IDS/IPS)** must be deployed at all network boundaries to inspect and filter inbound and outbound traffic.
- b. Firewall rules must follow a “deny-by-default” policy and be reviewed at least **quarterly** by the Security Manager.
- c. Administrative interfaces must not be exposed directly to the public internet.

3. Secure Configuration and Hardening –

- a. All servers, databases, and applications must be configured according to approved hardening baselines (e.g., CIS Benchmarks).
- b. Unnecessary services, ports, and default accounts must be disabled or removed.

- c. Configuration changes must be tracked in a version-controlled system and approved through the change-management process (see Section 7).

4. Patch and Vulnerability Management –

- a. Operating systems, firmware, and applications must be updated according to a defined patch schedule.
- b. Critical or high-severity vulnerabilities must be remediated within defined timelines or mitigated through compensating controls.
- c. Patch status must be reviewed monthly and documented by the IT Operations Team.

5. Remote-Access Security –

- a. Administrative access to internal systems must occur only through secure VPN channels protected by **multi-factor authentication (MFA)**.
- b. No direct administrator or database access is permitted from the public internet unless routed through a hardened **jump-host** or bastion server with full logging.
- c. Remote-access logs must be retained and reviewed per Section 12 – Monitoring, Logging and Audit.

6. DDoS Protection and Network Resilience –

- a. Network traffic must be continuously monitored for volumetric or protocol-based anomalies.
- b. DDoS-mitigation services and content-delivery networks (CDNs) must be implemented for external-facing assets.
- c. Redundant connectivity and failover routes must be configured to maintain service availability.

7. Cloud and Hosting Security –

- a. Cloud or hosting providers used for production environments must maintain recognized certifications such as **ISO 27001** or **SOC 2 Type II**.
- b. Access to cloud-management consoles must be limited to authorized personnel and protected by MFA.

- c. Network and resource configurations in cloud environments must be periodically reviewed for compliance with internal standards.

8. Logging and Monitoring –

- a. Network and system events must be logged and forwarded to the centralized log-management system (see Section 12).
- b. Logs must include timestamps, source and destination IPs, event types, and actions taken.
- c. Retention must comply with the company's defined policy and Curaçao AML/CFT record-keeping obligations.

9. Testing and Continuous Improvement –

- a. Regular internal and external vulnerability scans must be performed on network infrastructure.
- b. Lessons learned from incidents, audits, or penetration tests must be incorporated into updated configurations, rulesets, and monitoring thresholds.

10. Endpoint Protection and Operational Metrics –

- a. All endpoints and servers must run **Endpoint Detection and Response (EDR)** software integrated with the SIEM platform for centralized alerting.
- b. An **asset-discovery and CMDB reconciliation** process must operate continuously to identify unmanaged or rogue devices.
- c. All systems must maintain at least **90 % CIS benchmark conformance**; exceptions require documented compensating controls.
- d. The following **security KPIs** shall be tracked and reviewed quarterly:
 - 1. Mean Time to Respond (MTTR) for Priority-1 incidents
 - 2. Percentage of critical vulnerabilities remediated within defined SLA
 - 3. Phishing simulation failure rate
 - 4. Endpoint coverage and EDR alert closure rates.

These controls ensure that Games & More BV maintains a secure, resilient, and compliant infrastructure in accordance with Curaçao Gaming Authority requirements and recognized international cybersecurity standards.

7. Application and Game Engine Security

Games & More BV maintains strict security and quality-assurance controls across all internally developed and third-party applications, including game engines, player portals, back-office systems, and APIs.

This framework ensures that all software components operate securely, maintain data integrity, and uphold the fairness and transparency standards required by the Curaçao Gaming Authority (CGA).

1. Secure Development Lifecycle (SDLC) –

- a. All development activities must follow a defined SDLC incorporating security from design through deployment.
- b. Mandatory controls include peer code reviews, static and dynamic code analysis, dependency scanning for vulnerabilities, and secure build and deployment procedures.
- c. Open-source and third-party libraries must be continuously monitored for known vulnerabilities (e.g., via CVE databases or automated dependency-management tools).

2. Change-Management Controls –

- a. All changes to production systems must follow a documented change-management process that includes testing, peer review, management approval, rollback procedures, and post-deployment verification.
- b. Emergency changes must be logged, justified, and reviewed retrospectively within 24 hours.

3. Web Application and API Security –

- a. All public-facing applications must be protected by a **Web Application Firewall (WAF)** configured to detect and block common attack vectors such as SQL injection, XSS, and CSRF.
- b. APIs must enforce authentication, authorization, encryption in transit (TLS 1.2+), rate limiting, and periodic **API-key rotation**.

- c. Input validation and output encoding must be implemented to prevent injection or data-leakage vulnerabilities.

4. **Vulnerability Management and Penetration Testing –**

- a. Automated vulnerability scans must be conducted at least **quarterly**, with manual validation of high-risk findings.
- b. Independent third-party penetration tests must be performed at least annually or after significant platform updates.
- c. Results must be documented, prioritized by severity, and remediated within defined timeframes.
- d. All vulnerability-management activities must be overseen by the Security Manager and reviewed by the Compliance Officer.

5. **Random Number Generator (RNG) and Game-Integrity Assurance –**

- a. RNGs used in game engines must be certified by an **independent, recognized laboratory**, such as Gaming Labs International, eCOGRA, or BMM Testlabs, in accordance with international fairness standards.
- b. Certification reports and RNG-test results must be stored securely and retained for at least **five years**.
- c. Regular integrity checks must be conducted to confirm that deployed RNGs match the certified versions.

6. **Application Logging and Monitoring –**

- a. Application and game-engine logs must capture security-relevant events such as authentication failures, privilege escalations, and critical gameplay actions.
- b. Logs must be forwarded to the centralized logging platform described in **Section 12 – Monitoring, Logging and Audit** and retained per the defined retention policy.

7. **Secure Deployment and Configuration Management –**

- a. Production environments must be segregated from development and testing environments.

- b. Default credentials and sample configurations must be removed before deployment.
- c. Configuration changes must be version-controlled, reviewed, and documented.

8. Software Supply Chain Security

- a. All software components, libraries, and dependencies must be tracked through a **Software Bill of Materials (SBOM)** maintained within the SDLC toolchain.
- b. All builds must use **code-signing** and **secrets-scanning** to detect tampering or credential leakage.
- c. Build pipelines and third-party repositories must undergo review for integrity and provenance at least annually.
- d. Development, staging, and production environments must maintain **configuration parity** to reduce drift, enforced through **Infrastructure-as-Code (IaC)** and automated guardrails.
- e. Any configuration deviation detected must be logged, risk-assessed, and remediated promptly.

9. Continuous Improvement and Training –

- a. Developers and engineers must receive **secure-coding and application-security training** annually as part of the Information-Security Awareness Program (see Section 13).
- b. Lessons learned from incidents or penetration tests must feed back into coding standards and the SDLC process.

These controls ensure that all software and game-engine components developed or operated by Games & More BV remain secure, fair, and compliant with Curaçao Gaming Authority and international application-security standards.

8. Data Protection and Encryption

Games & More BV is committed to safeguarding all personal, financial, and operational data processed or stored within its systems.

This section defines the principles, technologies, and controls that ensure confidentiality, integrity, and availability of information in accordance with Curaçao Gaming Authority (CGA) requirements, the General Data Protection Regulation (GDPR), and other applicable laws.

1. Data Classification and Ownership –

- a. All information assets must be classified according to sensitivity (e.g., Public, Internal, Confidential, Highly Confidential).
- b. Each dataset must have a designated owner responsible for ensuring correct classification, access control, and handling procedures.

2. Encryption Standards –

- a. All data in transit must be encrypted using **TLS 1.2 or higher**, preferably **TLS 1.3**.
- b. All data at rest, including databases, file systems, and backups, must be encrypted using **AES-256 or equivalent industry-approved algorithms**.
- c. Encryption keys must be generated, stored, rotated, and retired in accordance with an approved **Key-Management Procedure**.

3. Storage and Handling of Sensitive Data –

- a. Personally identifiable information (PII), payment details, authentication credentials, and crypto-wallet keys must be stored only in encrypted or hashed form.
- b. Sensitive data must never be stored in plaintext, temporary files, or unsecured repositories such as shared drives or public cloud buckets.

4. Backup Strategy –

- a. Backups must be performed regularly and stored in **geo-redundant, encrypted** locations separate from production systems.
- b. Backup restoration tests must be performed at least **quarterly** to verify data integrity and recoverability.
- c. Backup retention must comply with **Curaçao AML/CFT** record-keeping obligations (minimum five years for transactional and gaming data).

5. Retention and Secure Deletion –

- a. Retention periods for player data, KYC documents, logs, and transactional records must be defined based on legal and business requirements.
- b. Data no longer required must be securely deleted or anonymized using industry-accepted destruction methods.
- c. A **Data-Retention Schedule** must be maintained and reviewed annually by the Compliance Officer.

6. Data Breach Response Procedures –

- a. Any suspected or confirmed data breach must follow the incident-management process defined in **Section 10 – Incident Response and Reporting**.
- b. The Incident Manager and Compliance Officer must coordinate detection, containment, investigation, and notification.
- c. Breaches involving personal data must be reported to relevant regulators (e.g., CGA, Data-Protection Authority) within prescribed timelines, typically **within 24 hours** of detection.

7. Third-Party Data Processing –

- a. Vendors or partners that process data on behalf of Games & More BV must provide written assurances of equivalent security and privacy controls.
- b. Data-processing agreements must include clauses for encryption, breach notification, and data-return or destruction upon termination.

8. Awareness and Training –

- a. All employees must receive data-protection awareness training as part of the Information-Security Awareness Program (see Section 13).
- b. Specialized training must be provided to staff handling KYC, payments, or technical operations to ensure proper data-handling practices.

9. Key Management –

- a. Encryption keys must be generated, stored, and managed within a dedicated **Hardware Security Module (HSM)** or **Cloud Key Management Service (KMS)** compliant with FIPS 140-2 Level 3 or higher.
- b. Access to encryption keys shall require **dual control** (two-person approval) and be logged in the centralized monitoring system.
- c. Keys protecting data at rest must be rotated at least annually or immediately after suspected compromise.
- d. Keys for crypto-wallets or high-value assets must use **Multi-Party Computation (MPC)** or cold-storage mechanisms, with offline backups stored in secure, geographically separated vaults.
- e. A **Key Lifecycle Register** must document key creation, distribution, rotation, and retirement events, reviewed quarterly by the Security Manager.

10. Data Subject Rights and Privacy Impact Assessments –

- a. Games & More BV shall maintain documented procedures for handling **Data Subject Requests (DSRs)** including access, rectification, erasure, restriction, and objection, in accordance with GDPR Articles 15–21.
- b. All verified DSRs must be acknowledged within 5 business days and fulfilled within the statutory timeframe.
- c. A **Data Protection Impact Assessment (DPIA)** must be conducted whenever new technologies, large-scale profiling, or cross-border data transfers are introduced.
- d. Records of Processing Activities (RoPA) shall be maintained by the Compliance Officer, reflecting all data categories, processing purposes, and retention schedules.

These data-protection measures ensure that Games & More BV upholds player privacy, secures operational data, and complies with Curaçao Gaming Authority and international information-security standards.

9. Business Continuity and Disaster Recovery (BC/DR)

Games & More BV maintains a comprehensive Business Continuity and Disaster Recovery (BC/DR) Framework to ensure the timely restoration of critical operations, systems, and services in the event of disruptions caused by technical failures, cyberattacks, or natural disasters.

The objective of this framework is to protect player interests, maintain regulatory compliance, and minimize operational and financial impact.

1. **Scope and Objectives** – The BC/DR Framework applies to all business functions, systems, and processes essential to the delivery of gaming services, including wallet systems, game engines, player account management, and compliance systems. Its primary goals are to ensure business continuity, protect data integrity, and restore services within acceptable timeframes.
2. **Recovery Objectives** –
 - a. **Recovery Time Objective (RTO):** The maximum acceptable time to restore a system or service after disruption.
 - b. **Recovery Point Objective (RPO):** The maximum acceptable amount of data loss measured in time.
Each critical system must have defined RTO and RPO values documented and approved by senior management and reviewed annually.
3. **Disaster Recovery Plan (DRP)** –
 - a. The DRP must outline the step-by-step recovery procedures for restoring systems, applications, and databases.
 - b. Recovery infrastructure must include an **alternative site or cloud region** with **geographic separation** from primary systems.
 - c. Cloud and hosting providers used for failover must hold recognized security certifications such as **ISO 27001** or **SOC 2 Type II**.

4. **Redundancy and High Availability** – Critical applications and databases must employ redundancy mechanisms such as hardware clusters, load balancers, replication, and automated failover to maintain uptime and prevent single points of failure.
5. **Data Backup and Restoration** –
 - a. Data backups must be performed according to a defined schedule and stored in **geo-redundant, encrypted** environments.
 - b. Backup integrity must be tested regularly through restoration exercises.
 - c. Backup retention must comply with **Curaçao AML/CFT** record-keeping requirements (minimum five years for transactional and gaming data).
6. **BC/DR Testing** –
 - a. The BC/DR plan must be tested at least **annually**, or more frequently following major system changes or incidents.
 - b. Each test must be **documented**, reviewed by the Compliance Officer, and any deficiencies tracked through corrective actions.
7. **Roles and Responsibilities** –
 - a. The **BC/DR Coordinator** oversees plan execution, testing, and documentation.
 - b. The **IT Operations Team** executes restoration activities and maintains technical readiness.
 - c. The **Compliance Officer** ensures the plan meets regulatory requirements and reports results to senior management.
8. **Communication and Escalation** – During a business disruption, clear communication lines must be maintained. The Incident Manager and Communications Lead (see Section 10 – Incident Response and Reporting) are responsible for internal updates and external notifications, including regulatory bodies if required.
9. **Integration with Risk Management** – Findings from BC/DR tests and real incidents shall feed into the company's risk register and be used to refine recovery procedures, enhance preventive controls, and update documentation.
- 10.

11. Quarterly Exercises and Post-Action Tracking –

- a. In addition to annual full recovery tests, **quarterly tabletop exercises** shall simulate disruptive scenarios (e.g., ransomware, cloud-region outage, or vendor failure).
- b. Findings, action items, and improvement tasks must be tracked through the **Corrective and Preventive Actions (CAPA)** process defined in Section 14 until closure.
- c. After-action reviews must document response effectiveness, communication clarity, and readiness metrics, feeding into the next BC/DR test plan and training cycle.

12. Reference Documentation – Refer to **Business Continuity Plan (BCP) Document v1.x** for detailed recovery scenarios, contact lists, escalation hierarchy, and test schedules supporting this section.

This framework ensures that Games & More BV can maintain essential operations and data integrity under all foreseeable conditions while meeting Curaçao Gaming Authority continuity requirements.

10. Incident Response and Reporting

Games & More BV maintains a structured Incident Response and Reporting Framework to ensure rapid detection, containment, investigation, and resolution of all security events that could affect player data, gaming integrity, or service availability.

The objective of this framework is to minimize impact, maintain regulatory compliance, and strengthen resilience through documented lessons learned.

1. Incident Response Team (IRT) Composition – An IRT shall be established and kept current. Roles include:

- **Incident Manager** – overall coordination, decision-making, escalation.
- **Forensics Lead** – evidence collection, analysis, and preservation.
- **Communications Lead** – manages internal and external communications.
- **Legal / Compliance Lead** – ensures reporting and documentation comply with Curaçao regulations and privacy laws.
Alternate personnel must be designated to guarantee 24/7 coverage.

2. Incident Classification – Security events must be categorized by severity and type to determine appropriate response levels:

- *Minor Incident* – limited impact, quickly contained (e.g., isolated malware detection).
- *Major Security Incident* – potential compromise of production systems or service availability.
- *Data Breach / PII Exposure* – unauthorized disclosure or access to personal or financial data.
- *Game-Integrity Incident* – manipulation or malfunction affecting fairness or RNG outcomes.

3. Incident Response Procedure – All incidents shall follow the defined lifecycle:
Identification → Triage → Containment → Investigation → Eradication → Recovery → Lessons Learned.

- Each phase must be documented within the incident-management system, including timestamps, responsible persons, and decisions taken.
4. **Evidence Handling and Chain of Custody** – All relevant logs, screenshots, and forensic images must be preserved in secure, tamper-evident storage. Evidence must be time-stamped, labeled, and traceable to maintain integrity and potential legal admissibility.
 5. **Internal Escalation and Communication** –
 - All personnel are responsible for immediately reporting suspected incidents to the Incident Manager or Security Manager.
 - The Incident Manager must notify the **Compliance Officer** and **senior management** without undue delay once a major or regulated incident is confirmed.
 - Communication with external parties, players, or media may only occur through the Communications Lead with management approval.
 6. **Regulatory and Legal Reporting Obligations** –
 - Incidents involving data compromise, service disruption, or integrity breaches must be reported to the **Curaçao Gaming Authority (CGA)** within the timeframes prescribed by license conditions (normally within 24 hours of detection).
 - Data breaches involving EU residents must also comply with **GDPR Article 33** notification requirements.
 - All regulatory correspondence must be recorded and retained as part of the incident file.
 7. **Post-Incident Review and Root-Cause Analysis** – After resolution, the IRT must conduct a debrief to identify contributing factors, evaluate response effectiveness, and define corrective and preventive actions. Outcomes must be documented and submitted to senior management.
 8. **Continuous Improvement and Integration** – Lessons learned from incidents shall feed directly into updates of the IT Security Protocol , staff training (see Section 13 – Policy and Awareness Training), and system monitoring enhancements (see Section 12 – Monitoring, Logging and Audit).

This framework ensures that Games & More BV can respond effectively to any security incident while maintaining player trust and full compliance with Curaçao Gaming Authority requirements.

11. Vendor and Third-Party Management

Games & More BV relies on multiple external partners – including payment processors, KYC/AML service providers, game studios, hosting platforms, and cloud vendors - to deliver secure and compliant gaming services.

This section defines the controls used to evaluate, approve, and continuously monitor all third-party relationships to ensure that vendor operations meet the company's information-security, privacy, and regulatory standards, and support continuous compliance.

1. **Vendor Inventory and Classification** – A maintained, up-to-date register of all third-party vendors and service providers must be kept. Vendors shall be classified according to criticality and data sensitivity (e.g., critical infrastructure, sensitive-data processors, non-critical suppliers).
2. **Pre-Contract Risk Assessment** – Before onboarding any vendor, a security and compliance due-diligence assessment must be performed to evaluate:
 - Information-security posture and incident history
 - Certifications (ISO 27001, SOC 2 Type II, PCI-DSS, or equivalent)
 - Data-protection compliance (e.g., GDPR)
 - Financial stability and jurisdictional suitability
 - Right-to-audit provisions and regulatory acceptability

All certifications and audit attestations must be verified for authenticity and expiry date prior to contract signing.

3. **Contractual Requirements** – All vendor agreements must include clauses covering:
 - Data-protection and confidentiality obligations
 - Notification of data breaches or security incidents within defined timelines
 - Right to audit and access compliance evidence

- Service-level agreements (SLAs) for uptime, response, and recovery
 - Data ownership, return, and destruction on contract termination
4. **Ongoing Vendor Monitoring** – The Compliance Officer and Security Manager shall jointly review vendor performance at least annually or more frequently for critical suppliers. Monitoring must include SLA compliance, incident reports, changes in certification status, and overall service reliability. Monitoring controls described in Section 12 support ongoing vendor oversight.
 5. **Incident Handling with Vendors** – Vendors must cooperate fully in incident investigations affecting shared systems or data. Incident-response coordination procedures must be defined contractually and aligned with **Section 10 – Incident Response and Reporting**.
 6. **Regulatory Compliance and Certifications** – For essential platform or game providers, verifiable certificates of compliance or independent lab testing (e.g., RNG, game fairness, payout validation) must be obtained, stored, and made available to the regulator upon request.
 7. **Termination and Offboarding** – Upon contract termination, vendors must securely delete or return all company or player data, confirm data destruction in writing, and revoke all system access credentials.
 8. **Third-Party Risk Review** – A summarized third-party risk assessment report shall be produced annually for management review and maintained as audit evidence.
 9. **Audit Rights and Notification Timelines** –
 - a. Games & More BV reserves the **right to audit** critical vendors with 10 business days' written notice, or immediately in the event of suspected breach or regulatory inquiry.
 - b. Vendors must notify Games & More BV of any **security incident or data breach within 24 hours** of discovery, providing initial impact details and remediation measures.
 - c. Vendor system access must undergo **re-certification every six months** to ensure least-privilege alignment and timely removal of obsolete accounts.

These vendor-management controls ensure that Games & More BV maintains oversight of all third-party relationships in accordance with Curaçao Gaming Authority requirements and international information-security standards.

12. Monitoring, Logging and Audit

To ensure continuous oversight, accountability, and regulatory compliance, Games & More BV maintains comprehensive monitoring, logging, and audit mechanisms across all production and back-office environments.

These controls support the detection of security events, the preservation of reliable gaming records, and the verification of system integrity for both internal management and external regulators.

1. **Centralized Logging** – All critical systems (servers, databases, game engines, transaction platforms, administrative portals) must forward logs to a centralized, access-controlled log management system. Logs must capture timestamps, event type, user or process ID, and originating system.
2. **Time Synchronization** – All systems that generate or store logs must synchronize their clocks with an authorized **NTP (Network Time Protocol)** server. This ensures event correlation and chronological integrity across infrastructure and audit records.
3. **Retention and Archiving** – Logs must be retained for a minimum of **twelve (12) months** in active storage and archived for at least **thirty-six (36) months** thereafter.

In accordance with Curaçao **AML/CFT** and gaming-record obligations, **transactional and gaming activity logs shall be retained for a minimum of five (5) years** from their creation date and remain readily accessible to the Compliance Officer and regulators upon request.

4. **Retention Review** – The Compliance Officer and Security Manager shall jointly review log-retention settings and archive accessibility at least once per year to confirm compliance with Curaçao's five-year gaming-record requirement.
5. **Security Event Management** – All logs are ingested into a **Security Information and Event Management (SIEM)** platform or equivalent solution capable of correlation, alerting, and trend analysis to detect potential threats in real time.

6. **Real-Time Monitoring and Alerts** – Automated monitoring tools shall generate alerts for anomalies such as unusual transaction volumes, repeated authentication failures, privilege escalation, administrative-account changes, or atypical crypto-wallet movements. Alerts must be reviewed promptly by the Security Manager or delegated analyst. Alerts indicating potential compromise or data exposure must trigger the procedures defined in **Section 10 – Incident Response and Reporting**.
7. **Integrity and Tamper Protection** – Log files and audit trails must be write-once or otherwise protected from alteration or deletion by standard users or administrators. Any attempted modification must itself be logged and reported. Log archives must be encrypted at rest (e.g., AES-256) and during transmission to off-site or cloud storage.
8. **Log Access Control** – Access to centralized logging and monitoring tools must be restricted to authorized personnel within the Security or Compliance teams. All access to log repositories must itself be logged and reviewed quarterly.
9. **Periodic Audits** – Internal security audits must be conducted at least annually to verify adherence to this protocol and evaluate control effectiveness. Independent external audits or certifications may be commissioned to validate compliance with the Curaçao CGA requirements and international standards (e.g., ISO 27001).
10. **Comprehensive Audit Trail** – A maintained audit trail shall include policy revisions, access-rights reviews, vendor and platform audits, and results of disaster-recovery or incident-response tests.
11. **Reporting and Continuous Improvement** – Findings from monitoring and audits must be documented, reported to senior management, and used to update security controls and training programs.

All monitoring, logging, and audit processes form part of Games & More BV's overall governance framework and shall be periodically reviewed to ensure alignment with evolving regulatory and technological standards.

13. Policy and Awareness Training

To maintain a strong security culture and ensure compliance with Curaçao regulatory standards, all employees, contractors, and key vendors of Games & More BV must receive structured information-security awareness and role-specific training.

The goal of this program is to ensure that every individual understands their responsibilities for protecting systems, player data, and confidential business information.

1. **Mandatory Onboarding Training** – All new staff must complete an Information-Security Awareness session within **30 days** of joining. Topics include password management, phishing prevention, data classification, acceptable-use rules, and incident-reporting procedures.
 - 1.1. The onboarding and training program shall be coordinated with the Human Resources department to ensure new hires cannot access production systems until mandatory training is completed.
2. **Annual Refresher Training** – All personnel must complete refresher training at least **once per year**. The training program must be updated regularly to reflect new threats, lessons learned from incidents, and regulatory changes.
3. **Role-Based Training** – Personnel with elevated privileges (e.g., system administrators, developers, database engineers) must receive tailored training covering secure coding, change-management, privileged-access controls, and handling of sensitive production data.
4. **Specialized Sessions** – Additional training shall be provided following major security incidents, audit findings, or technology changes to address identified gaps.
5. **Training Records and Evidence** – Attendance logs, completion certificates, and assessment results must be recorded and retained for at least **five years** to demonstrate compliance.
 - 5.1. The **Compliance Officer** is responsible for verifying completion and maintaining documentation.

5.2. Training effectiveness shall be evaluated through short quizzes or simulated phishing results, and overall completion rates shall be reviewed quarterly by the Compliance Officer.

6. **Policy Communication and Acknowledgement** – All staff must formally acknowledge that they have read and understood the company's IT Security Protocol and related procedures. Updated policies must be redistributed and acknowledged whenever significant revisions occur.

6.1. Refer also to **Section 14 – Compliance and Review** for actions applicable to non-compliance with mandatory training requirements.

7. **Continuous Awareness Initiatives** – Periodic awareness reminders (e-mails, posters, simulated phishing campaigns, internal newsletters) shall be used to reinforce good security habits and maintain vigilance.

This training framework forms part of Games & More BV's overall governance and compliance program and will be reviewed annually to maintain alignment with emerging threats and Curaçao Gaming Authority requirements.

14. Compliance and Review

To maintain alignment with Curaçao Gaming Authority (CGA) requirements and international best practices, Games & More BV shall implement a structured compliance and review process to ensure continuous improvement of its information-security posture.

1. **Annual Policy Review** – This IT Security Protocol and associated procedures must be reviewed at least **once per year**, or sooner if significant changes occur (e.g., introduction of new technologies, regulatory amendments, or major organizational changes). The review process shall verify continued adequacy, relevance, and effectiveness.
 - 1.1. Policy reviews must also consider the most recent risk-assessment results and any emerging threats identified under Section 4 – Risk Assessment and Asset Inventory.
2. **Change-Triggered Review** – Interim reviews must be initiated following material changes such as system migrations, the introduction of new vendors, the addition of new game platforms, or major security incidents.
3. **Compliance Monitoring** – The **Compliance Officer** is responsible for monitoring adherence to this policy's protocol, performing periodic internal checks, and ensuring that deviations or deficiencies are identified, documented, and remediated.
4. **Management Oversight** – A summary of compliance activities, key findings, and corrective actions shall be presented to **senior management** at least annually. Management is responsible for ensuring that adequate resources are allocated to maintain compliance.
5. **Corrective and Preventive Actions (CAPA)** – Any non-compliance or audit finding must be addressed through a formal corrective action plan. Actions shall include root-cause analysis, defined responsibilities, and target completion dates. Preventive measures should be recorded to mitigate the recurrence of similar issues.

6. **Regulatory Reporting** – Significant breaches of policy’s protocol or material non-compliance that may affect data integrity, player protection, or system availability must be reported to the **Curaçao CGA** within the timelines prescribed by the license conditions or local law.
7. **Continuous Improvement** – The results of reviews, audits, and incident analyses shall feed into a continuous-improvement process. Updates and lessons learned must be incorporated into subsequent policy’s protocol revisions and staff awareness programs.
8. **Documentation Control** – All reviews and updates of this policy must be version-controlled, approved by senior management, and logged in the document revision history.
9. **Policy Enforcement** – All employees, contractors, and vendors must comply with this IT Security Protocol. Non-compliance may result in disciplinary action up to and including contract termination. Repeated or deliberate violations will be escalated to senior management and may be reported to the Curaçao Gaming Authority (CGA) if they impact regulatory obligations.
10. **Exception Management** – Occasional deviations from the policy’s protocol may be approved where justified by business or technical necessity and where compensating controls maintain equivalent risk reduction;
 - a. Exceptions must be formally requested using the Security Exception Form.
 - b. All requests must document the reason, scope, affected systems, temporary controls, and expiry date.
 - c. Approvals require joint sign-off by the **CTO** and **Compliance Officer**, with input from the **Security Manager**.
 - d. Exceptions must specify a maximum validity period of 90 days (renewal requires re-approval).
 - e. An **Exceptions Register** shall be maintained by the Compliance Officer, reviewed quarterly, and presented to senior management during policy/protocol reviews.

This review process ensures that Games & More BV maintains a proactive compliance posture and upholds the security and integrity obligations defined by the Curaçao Gaming Authority.

Appendix A – Abbreviations and Definitions

Term / Acronym	Meaning / Definition
CGA	Curaçao Gaming Authority – the official national regulatory authority overseeing gaming compliance and licensing
AML/CFT	Anti-Money Laundering / Combating the Financing of Terrorism regulations applicable under Curaçao law.
ISO 27001 / 27002	International standards defining information-security management systems (ISMS) and best practices.
ISO 22301	International standard for Business Continuity Management Systems.
BCP / BC/DR	Business Continuity Plan / Business Continuity and Disaster Recovery – frameworks ensuring operational resilience during disruptions.
SIEM	Security Information and Event Management system for centralised log correlation, alerting, and threat detection.
NTP	Network Time Protocol – ensures synchronised timestamps across systems and logs.
MFA	Multi-Factor Authentication – security mechanism requiring multiple verification factors for system access.
PAM	Privileged Access Management – system controlling, monitoring, and auditing elevated user accounts.
RTO / RPO	Recovery Time Objective / Recovery Point Objective – metrics defining acceptable downtime and data-loss limits.
RNG	Random Number Generator – cryptographically secure mechanism used to ensure fairness in games.
WAF	Web Application Firewall – security layer protecting web apps from injection, XSS, and other attacks.
IDS/IPS	Intrusion Detection / Prevention System – tools for monitoring and blocking malicious network activity.

PII	Personally Identifiable Information – any data that can directly or indirectly identify a player or individual.
GDPR	General Data Protection Regulation (EU) – European regulation governing the processing and protection of personal data.
CVE	Common Vulnerabilities and Exposures – public database of known security vulnerabilities.
CAPA	Corrective and Preventive Actions – documented process for addressing and preventing compliance issues.
CTO	Chief Technology Officer – senior executive responsible for IT governance and security oversight.
SOC 2 Type 2	System and Organization Controls Type II – independent audit reports confirming service-provider security and compliance.
TLS	Transport Layer Security – cryptographic protocol securing data in transit over networks.
AES-256	Advanced Encryption Standard (256-bit) – industry standard for encrypting data at rest.

Appendix B – Reference Documents

1. ISO 27001:2022 – Information Security Management Systems (ISMS) Requirements
2. ISO 27002:2022 – Information Security Controls
3. ISO 22301:2019 – Business Continuity Management
4. Curaçao Gaming Control Board (GCB) – Technical & Regulatory Guidelines
5. Curaçao Gaming Authority (CGA) – Technical & Regulatory Guidelines
6. National Ordinance on Games of Chance (NOGC)
7. AML/CFT Guidelines for Gaming Operators (Curaçao)
8. GDPR (EU Regulation 2016/679)
9. NIST SP 800-61 r2 – Computer Security Incident Handling Guide
10. CIS Benchmarks – System Hardening Standards

Appendix C – Document Control

Version	Date	Description / Changes	Approved By
1.0	01/01/2025	Initial release	CTO – Raymond Saliba
1.1	01/08/2025	Updated to include Sections 4-14; aligned with ISO 27001 controls and CGA guidelines	CTO – Raymond Saliba
1.2	01/10/2025	Added key-management, supply-chain, metrics, and exception-handling enhancements; aligned password and privacy controls with current best practices.	CTO – Raymond Saliba

Appendix D – Policy Acknowledgement Form

Fill in this form to acknowledge the reading, understanding and implementation of this protocol.

Policy Title:	IT Security Protocol (v1.2)
Employee Name:	
Role/Department:	
Date Received:	
I acknowledge that I have read, understood, and agree to comply with the IT Security Protocol and related procedures. I understand that violations may result in disciplinary action per Section 14.	
Signature:	Date:
Signature:	Date: