

INFORMATION SECURITY POLICY

MuchGaming B.V.

operating as Crypto.Games

License Number	OGL/2024/1336/1047
Licensing Authority	Curaçao Gaming Authority (CGA)
Registered Entity	MuchGaming B.V.
Registered Office	Korporaalweg 10, Willemstad, Curaçao
Chamber of Commerce No.	153126
Platform	Crypto.Games (https://crypto.games)
Document Version	1.0
Effective Date	May 2026
Next Review Date	May 2027
Approving Authority	Board of Directors, MuchGaming B.V.
Responsible Officer	Board of Directors
Document Classification	Internal — Restricted

Prepared pursuant to the Curaçao National Ordinance on Games of Chance (LOK), the CGA Licensing and Operational Requirements (2025), and the National Ordinance on Personal Data Protection (LBP) .

1. Policy Statement

MuchGaming B.V. (**the Company, we, us, our**), incorporated in Curaçao under Chamber of Commerce number 153126 and operating the online gaming platform **Crypto.Games** (the “Platform”) under licence OGL/2024/1336/1047 issued by the Curaçao Gaming Authority (the “**CGA**”), is committed to protecting the confidentiality, integrity and availability of all information assets entrusted to it by its players, employees, regulators, business partners, and the public.

The Company recognises that information security is a foundational requirement for an online gaming operator. The integrity of game outcomes, the protection of player funds, the safeguarding of personal data and the continuous availability of the Platform are inseparable from the security controls described in this Information Security Policy (the “Policy”). A failure of any one of those areas materially threatens player trust, the Company’s licence to operate, and the Curaçao licensing regime as a whole.

This Policy establishes the principles, governance, controls and accountabilities by which the Company identifies, assesses, mitigates and monitors information security risks across all of its systems, premises and personnel. It applies a risk-based approach: controls are deployed proportionately to the sensitivity of information assets and to the threats faced by the Platform, with particular emphasis on player personal data, financial and crypto-asset transaction data, gaming system integrity, and operational resilience.

The Board of Directors of MuchGaming B.V. has formally approved this Policy and is ultimately accountable for its enforcement. The Management is responsible for its day-to-day implementation, maintenance and monitoring. All directors, officers, employees, contractors and agents of the Company are required to comply with this Policy and to support the information security program it establishes.

2. Purpose

The purpose of this Policy is to:

- Establish a comprehensive information security framework that meets the legal and licensing requirements applicable to MuchGaming B.V. under the laws of Curaçao and the standards of the CGA;
- Protect the confidentiality, integrity and availability of all information processed, stored or transmitted by, or on behalf of, the Company;
- Protect player personal data in accordance with the Curaçao National Ordinance on Personal Data Protection (Landsverordening bescherming persoonsgegevens — “LBP”) and, where applicable, the EU General Data Protection Regulation (Regulation (EU) 2016/679 — “GDPR”);
- Protect the integrity of the gaming system, including random number generation, game logic, payout records, wallet operations and financial reconciliation, in line with the technical and operational requirements of the CGA;

- Define clear roles, responsibilities, accountabilities and reporting lines for information security across the Company;
- Ensure that information security risks are identified, assessed, treated and monitored on a continuous basis through a documented information security program ;
- Establish controls for the prevention, detection, response to and recovery from information security incidents, including cyber-attacks, data breaches and operational disruptions;
- Ensure that third parties acting on behalf of the Company (including game suppliers, payment and on-ramp providers, KYC/AML vendors, cloud infrastructure providers and outsourced support) are subject to security requirements consistent with this Policy; and
- Foster a strong, sustained culture of information security awareness and accountability among all personnel.

3. Scope and Audience

3.1 Material Scope

This Policy applies to all information assets that are owned, controlled, processed or stored by the Company, regardless of format or location. This includes, without limitation:

- All electronic information processed by the Platform, including player accounts, wallet records, gameplay data, transaction history, KYC/AML records, support and complaint files, marketing and preference data, and technical logs;
- All physical records (including printed documents, identity-document copies retained where lawful, and any portable media) generated or held by the Company;
- All information systems, applications, databases, networks, cloud environments, devices, virtual machines, code repositories and infrastructure on which the Platform depends;
- All on-premises premises and remote-working arrangements used by personnel of the Company; and
- All information shared with third parties acting on behalf of the Company, irrespective of the geographic location of those third parties.

3.2 Personal Scope

This Policy applies to:

- All directors, officers and members of the management of MuchGaming B.V.;
- All employees, whether full-time, part-time, fixed-term or temporary;
- All consultants, contractors, agents and outsourced service providers acting on behalf of the Company; and
- All other persons who are granted access to the Company's information, systems or premises.

All such persons are referred to in this Policy as "Personnel". All Personnel are responsible for compliance with this Policy. Failure to comply may result in disciplinary action up to and including termination of employment or contract, and may give rise to civil or criminal liability.

3.3 Excluded Matters

This Policy does not address matters that are governed exclusively by other policies of the Company, including the AML/CFT Policy, the Privacy Policy, the Responsible Gaming Policy, the Self-Exclusion Policy, the Player Complaints & Dispute Resolution Policy and the Code of Conduct. Where there is overlap, this Policy applies in addition to those policies; in the event of any conflict in respect of personal data handling, the Privacy Policy prevails.

4. Definitions

For the purposes of this Policy, the following terms have the meanings set out below. Capitalised terms not defined here have the meaning given to them in the Company's Terms & Conditions or in the applicable Curaçao legislation.

Asset	Anything that has value to the Company, including information, software, hardware, services, people and premises.
Availability	The property of being accessible and usable upon demand by an authorised entity.
CGA	The Curaçao Gaming Authority, the public authority responsible for the licensing and supervision of online gaming operators in Curaçao.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
Control	A measure that modifies risk, including policies, procedures, technical measures, organisational structures and physical safeguards.
Data Subject	An identified or identifiable natural person to whom personal data relates.
Information security program	The information security program established and maintained by the Company in accordance with this Policy.
Incident	A single or series of unwanted or unexpected information security events that has a significant probability of compromising business operations or threatening information security.
Information Asset	Any data, document or system, in any form, that is of value to the Company and that requires protection.
Integrity	The property of accuracy and completeness of information and processing methods.
LBP	The Curaçao National Ordinance on Personal Data Protection (Landsverordening bescherming persoonsgegevens).
LMOT	The Curaçao National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties).
LOK	The Curaçao National Ordinance on Games of Chance (Landsverordening op de kansspelen), as amended.

Personal Data	Any information relating to a Data Subject, as further defined in the LBP and the GDPR (where applicable).
Personnel	Any person performing work for or on behalf of the Company, as further defined in Section 3.2.
Platform	The online gaming platform operated by the Company at https://crypto.games and any related domains.
Player	A natural person who has registered an Account on the Platform.
Risk	The effect of uncertainty on the Company's information security objectives, expressed as a combination of likelihood and impact.
Risk Owner	The person accountable for managing a particular risk and the controls that mitigate it.
Third Party	Any external organisation that processes information on behalf of the Company or that has access to the Company's information systems or premises.

5. Information Security Governance

5.1 Governance Principles

Information security at the Company is governed by the following principles:

- **Accountability:** information security responsibilities are documented and assigned to identified individuals at every level of the organisation.
- **Risk-based:** security investments and controls are determined by a documented assessment of threats, vulnerabilities and impacts to the Company's objectives, with particular regard to player protection and licence-critical processes.
- **Defence in depth:** the Company applies multiple, overlapping layers of administrative, technical and physical controls so that the failure of any single control does not result in a material compromise.
- **Least privilege and need to know:** access to information assets is granted only to the extent required to perform an authorised task.
- **Separation of duties:** no individual has end-to-end control of a critical process where that would create an unacceptable risk of error, fraud or abuse.
- **Continuous improvement:** the Company monitors the effectiveness of its controls and updates them in response to new threats, incidents, audit findings and regulatory changes.
- **Transparency:** the Company maintains documented policies and procedures, retains evidence of compliance, and cooperates fully with the CGA and other competent authorities.

5.2 Roles and Responsibilities

5.2.1 Board of Directors

The Board of Directors of MuchGaming B.V. has ultimate accountability for information security. The Board:

- approves this Policy and any material amendments to it;
- approves the Company's information security risk appetite and risk tolerance thresholds;
- ensures that adequate financial, technical and human resources are allocated to information security; and
- receives, at least annually, a written report on the state of the information security program, on the most significant risks and on any material incidents that occurred during the period.

5.2.2 AML Officer

The AML Officer coordinates with Management on matters at the intersection of information security and AML/CFT compliance, including data handling and integrity controls.

5.2.3 IT and Operations Management

IT and Operations Management implement, operate and monitor the technical controls described in this Policy and its supporting standards, including identity and access management, network security, system hardening, logging and monitoring, vulnerability management, backup and recovery, and change management.

5.2.4 Department Heads and Line Managers

Each department head and line manager is responsible for ensuring that the Personnel under their supervision: (i) understand this Policy; (ii) complete required information security training; (iii) follow the procedures applicable to their role; and (iv) report any actual or suspected information security incident promptly through the channels described in Section 16.

5.2.5 All Personnel

Every member of Personnel is personally responsible for protecting the information assets to which they have access, for using systems and credentials only for authorised purposes, and for reporting any suspected security weakness or incident.

5.3 Information Security Program

The Company maintains a documented information security program maintained. The information security program is the structured set of policies, procedures, processes, records and tools through which the Company manages information security on a continuous basis. The information security program includes, at a minimum:

- This Policy and supporting topic-specific policies, standards, procedures and guidelines;
- The information security risk management framework described in Section 5.4;
- The control set described in Sections 6 to 18;
- Records of risk assessments, internal audits, management reviews, incidents, training, third-party assessments and corrective actions; and

- A defined annual review cycle and a process for ad-hoc updates following incidents, audits or significant changes.

5.4 Risk Management Framework

The Company manages information security risk on a continuous basis through a documented risk-management process. The process comprises the following steps:

1. Context establishment — defining the internal and external context, the scope of the assessment, the assets concerned and the risk-acceptance criteria approved by the Board.
2. Risk identification — identifying threats, vulnerabilities, existing controls, and the realistic scenarios in which a compromise of confidentiality, integrity or availability could occur.
3. Risk analysis — assessing the likelihood and impact of each scenario, taking into account the specific characteristics of an online crypto-gaming operator (e.g., wallet drains, RNG manipulation, account takeover, payment-rail abuse, regulatory exposure).
4. Risk evaluation — comparing the analysed risks against the Company's risk appetite to determine which require treatment.
5. Risk treatment — selecting and implementing appropriate controls, transferring the risk (e.g., through insurance), avoiding the risk, or accepting the risk subject to documented sign-off by the relevant Risk Owner and, for residual risks above the Board's tolerance, by the Board itself.
6. Monitoring and review — tracking the effectiveness of the controls, the emergence of new threats, the status of treatment plans, and the residual risk profile.

The risk register is maintained by Management, reviewed at least quarterly by senior management, and reported to the Board at least annually and immediately following any material incident.

6. Information Asset Management

6.1 Asset Inventory

The Company maintains, and Management maintains a comprehensive inventory of information assets. The inventory records, for each asset: (i) a unique identifier; (ii) a description; (iii) the Asset Owner; (iv) the Risk Owner (where different); (v) the data classification; (vi) the location and processing environment; (vii) the dependencies on other assets; and (viii) any applicable retention period. The inventory is reviewed at least annually and on every material change.

6.2 Asset Ownership

Every information asset has a single named Asset Owner. The Asset Owner is accountable for: (i) classifying the asset; (ii) ensuring that appropriate controls are in place; (iii) authorising access; (iv) reviewing access rights periodically; and (v) approving the disposal of the asset at the end of its retention period.

6.3 Acceptable Use

Personnel may use information assets only for legitimate business purposes and in accordance with the Company's Acceptable Use Standard. The Acceptable Use Standard prohibits, without limitation: (i) the storage of player personal data on personal devices or unauthorised cloud services; (ii) the use of Company credentials on personal accounts or services; (iii) the bypassing or disabling of security controls; and (iv) the introduction of unlicensed or unauthorised software.

6.4 Return and Disposal of Assets

All information assets in the custody of a member of Personnel must be returned to the Company on termination of employment or contract or on request from Management. Information assets that are no longer required must be disposed of using methods that prevent the recovery of any sensitive information, including secure wiping, cryptographic erasure or physical destruction, as appropriate to the classification of the asset.

7. Data Classification and Handling

7.1 Classification Scheme

All information processed by the Company is classified according to the following four-level scheme:

Classification	Description	Examples
Public	Information that has been formally approved for public release. Disclosure is not expected to harm the Company.	Marketing materials, public Terms & Conditions, the Privacy Policy on the Platform.
Internal	Information not intended for public release but the unauthorised disclosure of which would have limited adverse effect.	Internal procedures, organisation charts, non-sensitive operational documents.
Confidential	Information whose unauthorised disclosure would harm the Company, its players, partners or Personnel.	Player personal data, KYC documents, transaction logs, source code, contractual terms with third parties.
Restricted	Information whose unauthorised disclosure would cause severe harm, including regulatory action, material financial loss or harm to a player.	Production cryptographic keys, RNG seeds and configurations, hot-wallet credentials, AML investigation files, security incident details, security architecture diagrams.

7.2 Handling Rules

Management maintains a Data Handling Standard that prescribes, for each classification level, the rules for: (i) labelling; (ii) storage; (iii) access; (iv) transmission; (v) printing and physical distribution; (vi) backup; and (vii) disposal. Restricted and Confidential information must be encrypted in transit

using up-to-date TLS configurations and encrypted at rest using industry-standard algorithms (see Section 9).

7.3 Player Personal Data

Player personal data is, by default, classified as Confidential. KYC documents, sanctions and PEP screening records, source-of-funds evidence and other AML files are classified as Restricted. The processing of player personal data is governed by the Privacy Policy and the LBP, and (where applicable) by the GDPR. Management ensures that technical and organisational measures appropriate to the risk are implemented, including pseudonymisation, encryption, access controls, audit logging, and the principles of data minimisation and storage limitation.

7.4 Data Retention and Disposal

The Company retains personal and transactional data only for as long as necessary to fulfil the purpose for which it was collected, to comply with legal and regulatory obligations (in particular under the LOK, the LMOT and AML/CFT requirements), to defend against legal claims, or to enforce its agreements. Specific retention periods are set out in the Privacy Policy and the AML/CFT Policy. On expiry of the applicable retention period, data is deleted or anonymised in accordance with the Data Handling Standard.

8. Access Control

8.1 Access Control Principles

Access to information, systems and premises is granted on the basis of business need, the principle of least privilege, and segregation of duties. Access rights are formally requested, approved by the relevant Asset Owner, recorded, periodically reviewed and promptly revoked when no longer required.

8.2 User Access Management

- Each user is assigned a unique user identifier. Shared, generic or anonymous accounts are not permitted on production systems, except for tightly controlled break-glass accounts whose use is fully logged and reviewed.
- New access requests follow a documented joiner-mover-leaver process. Access for new joiners is provisioned only after a signed contract, completion of pre-employment screening (where required) and acknowledgement of this Policy.
- Changes in role or responsibility trigger a review and adjustment of access rights to align with the new function (mover process).
- Access is revoked on the same business day on which a person leaves the Company or on which a contract is terminated; access for personnel on long-term leave is suspended.
- Access rights to systems holding Confidential or Restricted information are reviewed at least every six months by the relevant Asset Owner.

8.3 Authentication

- All access to Company systems requires authentication. Passwords must comply with the Authentication Standard, including minimum length, complexity, rotation rules where appropriate, and protection against brute-force attacks.
- Multi-factor authentication (MFA) is mandatory for: (i) all administrative or privileged access; (ii) all remote access to Company networks; (iii) access to systems processing Confidential or Restricted information; (iv) access to wallet, payment and treasury systems; and (v) access to the player administration back-office.
- Personnel must not share, write down or otherwise disclose authentication credentials. Credentials suspected of being compromised must be reset and reported to Management immediately.

8.4 Privileged Access

Privileged access (such as administrator, root, database owner, cloud-tenant owner and security-tool administrator access) is tightly controlled. Privileged accounts:

- are individually attributable;
- are protected with MFA and, where supported, with just-in-time elevation;
- are subject to enhanced logging that cannot be modified by the privileged user themselves;
- are reviewed at least quarterly; and
- are managed through a privileged access management (PAM) solution where technically feasible.

8.5 Remote Access and Endpoint Posture

Remote access to Company systems is permitted only over encrypted channels (TLS or VPN), from devices that meet the Endpoint Security Standard (current operating-system patches, full-disk encryption, host-based anti-malware, screen-lock and host-based firewall enabled), and only after MFA. Personally owned devices may be used only where explicitly authorised by Management and only with appropriate technical controls (e.g., containerisation).

8.6 Player Account Security

The Platform implements security controls to protect Player Accounts, including, at a minimum: (i) strong password requirements and protection against credential stuffing; (ii) optional or, for higher-risk operations, mandatory two-factor authentication; (iii) anomaly detection on logins (e.g., new device, new IP, unusual geolocation); (iv) session timeouts and re-authentication requirements for sensitive actions such as withdrawals and changes of withdrawal address; (v) lock-out and notification mechanisms following multiple failed login attempts; and (vi) Player-facing security guidance in the help centre.

9. Cryptography and Key Management

9.1 Cryptographic Controls

The Company uses cryptography to protect the confidentiality, integrity and authenticity of information. Cryptographic mechanisms must be selected from the algorithms and parameters approved in the Company's Cryptography Standard, which is reviewed at least annually and updated to reflect current best practice and the recommendations of recognised authorities (e.g., NIST, ENISA, IETF).

- Confidential and Restricted data is encrypted in transit using current TLS versions with strong cipher suites; deprecated protocols and ciphers are explicitly disabled.
- Confidential and Restricted data is encrypted at rest using authenticated encryption with industry-accepted algorithms (e.g., AES-256-GCM).
- Passwords are stored using salted, adaptive password-hashing algorithms (e.g., Argon2id or bcrypt) with parameters reviewed periodically.
- Internal service-to-service communication is mutually authenticated using certificates issued by the Company's internal certificate authority where technically feasible.

9.2 Key Management

Cryptographic keys are managed throughout their lifecycle (generation, distribution, storage, rotation, archival and destruction) in accordance with the Key Management Standard. Production keys are generated within hardware security modules (HSMs) or equivalent key-management services and are never exposed in clear text outside of those environments. Access to production keys is restricted to a small number of named individuals subject to dual-control where appropriate, and is fully audited.

9.3 Crypto-Asset Wallet Security

Given the crypto-asset focus of the Platform, wallet security is a Restricted-class control. The Company segregates customer funds in cold-storage wallets to the maximum extent operationally feasible, with only operationally necessary balances held in hot wallets. Withdrawals from cold storage require multi-party approval. Hot-wallet keys are stored in HSMs or equivalent secure environments, with strict transaction limits, allow-listing of withdrawal addresses where appropriate, and continuous balance monitoring with alerting.

9.4 Random Number Generation and Game Integrity

The Company uses certified random number generators (RNGs) and provably-fair mechanisms to ensure the integrity of game outcomes. RNG seeds, configurations and audit reports are classified as Restricted. Any change to game logic or RNG configuration is subject to formal change control (Section 10.1), independent testing, and — where required by the CGA — re-certification by an accredited testing laboratory.

10. Operations Security

10.1 Change Management

All changes to information systems, including code releases, configuration changes, and infrastructure changes, are subject to documented change management. Each change is: (i) requested through a tracked record; (ii) risk-assessed; (iii) peer-reviewed; (iv) tested in a non-production environment; (v) approved by an authorised change approver; (vi) implemented in line with a defined deployment plan; and (vii) verified post-implementation. Emergency changes follow an expedited procedure with retrospective management review.

10.2 Separation of Environments

Development, testing, staging and production environments are logically and, where appropriate, physically separated. Production data, including player personal data, must not be used in non-production environments unless it has been irreversibly anonymised in accordance with the Data Handling Standard.

10.3 Capacity, Performance and Availability

The Company monitors system capacity, performance and availability to support the operational continuity of the Platform. Capacity forecasts and performance baselines are reviewed at least quarterly. Service level objectives for licence-critical services (including authentication, deposits, withdrawals, gameplay and the regulator-facing reporting interface) are documented, monitored and reported.

10.4 Logging and Monitoring

Security-relevant events on all production systems are logged centrally to a tamper-resistant logging facility. At a minimum, the Company logs: (i) authentication events and authorisation decisions; (ii) administrative and privileged actions; (iii) access to player personal data and AML files; (iv) wallet and treasury operations; (v) changes to game configuration; and (vi) security alerts from network and endpoint controls. Logs are retained for the period required by the LOK, the LMOT and the LBP, and reviewed in accordance with the Logging and Monitoring Standard. Personnel must not attempt to disable, modify or delete log entries.

10.5 Vulnerability and Patch Management

The Company operates a continuous vulnerability management programme that includes: (i) authenticated and unauthenticated vulnerability scans of internal and external assets at intervals defined in the Vulnerability Management Standard; (ii) participation in vendor advisory channels; (iii) prioritisation based on exploitability and asset criticality; (iv) defined remediation timelines (e.g., critical: 7 days; high: 30 days; medium: 90 days); and (v) at least annual independent penetration testing of the Platform and supporting infrastructure, with findings tracked through to closure.

10.6 Anti-Malware

Endpoints and servers run reputable, centrally managed anti-malware and endpoint detection and response (EDR) tooling with up-to-date signatures and behavioural detection capabilities. Personnel must not disable these tools and must report any alert to Management.

10.7 Backup and Recovery

Backups of player, transactional, configuration and supporting data are performed on a defined schedule. Backups are encrypted, integrity-checked, and stored in geographically separate locations from the primary data. Backup restoration is tested at least annually for licence-critical systems. Recovery point objectives (RPOs) and recovery time objectives (RTOs) are defined per service in the Business Continuity Plan (Section 14).

10.8 Network Security

- Production networks are segmented based on trust zones (e.g., public-facing, application, database, management, wallet/treasury), with traffic between zones controlled by stateful firewalls and, where appropriate, by intrusion prevention systems.
- Public-facing services are protected by a web application firewall (WAF) and by anti-DDoS measures appropriate to the size and exposure of the Platform.
- Administrative interfaces of network devices and infrastructure are not exposed to untrusted networks and require MFA.
- Wireless networks used for business purposes are encrypted and authenticated; guest networks are isolated.

10.9 Secure Configuration and Hardening

Servers, network devices, databases, cloud resources and endpoints are configured according to documented hardening baselines aligned with recognised benchmarks (e.g., CIS Benchmarks). Compliance with the baselines is monitored continuously where technical means allow, and deviations are tracked as exceptions through the risk-management process.

11. Secure Development and Maintenance

11.1 Secure Software Development Lifecycle

Software developed by or for the Company follows a documented Secure Software Development Lifecycle (SSDLC). The SSDLC integrates security throughout the lifecycle, including: (i) security requirements derived from this Policy and from applicable regulatory obligations; (ii) threat modelling for material new features and architectural changes; (iii) secure coding standards (including OWASP guidance); (iv) static and dynamic application security testing in the build pipeline; (v) software composition analysis to manage vulnerabilities in open-source dependencies; (vi) peer code review with security as an explicit review criterion; and (vii) pre-release security validation.

11.2 Secrets Management

Application secrets (including API keys, service credentials, signing keys and tokens) must not be hard-coded, committed to source-code repositories or shared through unsecured channels. Secrets are stored in approved secrets-management systems, rotated regularly, and access to them is logged.

11.3 Outsourced Development

Where development is outsourced to a third party, the contract incorporates security requirements consistent with this Policy, code-ownership and source-availability terms, and the right to perform security testing of the delivered code. The Company performs its own security validation prior to deployment, regardless of any assurances provided by the supplier.

12. Supplier and Third-Party Security

12.1 Risk-Based Due Diligence

Before engaging a third party that will process Company information or have access to Company systems, the Company performs a risk-based due-diligence assessment proportionate to the sensitivity of the information involved and the criticality of the service. The assessment considers, as applicable, the third party's certifications (e.g., SOC 2), independent audit reports, the location of processing, sub-processor arrangements, incident history, and financial standing.

12.2 Contractual Requirements

Contracts with third parties processing Confidential or Restricted information include, as a minimum:

- Confidentiality undertakings;
- A description of the permitted purposes and processing activities;
- Specific information security requirements aligned with this Policy;
- Data protection clauses meeting the LBP and, where applicable, the GDPR (including standard contractual clauses for international transfers);
- Notification obligations in respect of information security incidents and personal data breaches, with defined timelines;
- Audit rights for the Company and, where applicable, for the CGA and other competent authorities;
- Sub-processor approval and flow-down obligations;
- Service levels and exit/termination assistance, including the secure return or deletion of Company information.

12.3 Ongoing Oversight

The Company maintains a register of third parties processing Company information. Management reviews material third parties at least annually, taking into account changes in the service, in the regulatory environment, and in the threat landscape.

13. Physical and Environmental Security

Physical access to Company premises and to facilities housing Company information assets is controlled. Where the Company operates its own premises, the following controls apply, supplemented by the controls of any cloud or hosting provider for facilities operated by such provider:

- Defined secure perimeters with appropriate physical barriers and access controls;

- Identification and access authorisation for all persons entering the premises, including visitors;
- Visitor escorts and visitor access logs;
- Protection of areas containing sensitive information or critical infrastructure (e.g., wiring closets, comms rooms) by additional access controls;
- CCTV surveillance of perimeters and sensitive areas where lawful and proportionate;
- Environmental controls (fire detection and suppression, climate control, water-leak detection, surge protection) appropriate to the sensitivity of the equipment;
- Clear-desk and clear-screen practices for all Personnel handling Confidential or Restricted information; and
- Secure disposal of paper records and physical media containing sensitive information.

14. Business Continuity and Disaster Recovery

The Company maintains a documented Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) designed to ensure the continuity of licence-critical services and the protection of player funds and personal data in the face of disruptive events. The BCP and DRP cover, without limitation:

- A business impact analysis identifying critical processes, dependencies, RTOs and RPOs;
- Plans for the recovery of IT infrastructure, applications, data and connectivity, including failover, geographic redundancy and the restoration of backups;
- Plans for personnel safety, communications and remote-working continuity;
- Player communications protocols during a disruption;
- Notification protocols for the CGA, the Office for Personal Data Protection and other competent authorities, where relevant;
- A schedule of testing exercises (including at least one full or partial recovery exercise per year for licence-critical services), with documented results and improvement actions; and
- Periodic review of the BCP and DRP, and updates following any significant change to the Platform or to the Company's operations.

15. Human Resources Security

15.1 Pre-Employment

Candidates for positions involving access to Confidential or Restricted information are subject to background verification proportionate to the sensitivity of the role and to the requirements of the LOK and the CGA. Verification may include, where lawful: identity verification, employment history, education, criminal records, financial-soundness checks (for treasury or finance roles), and references.

15.2 Terms of Employment

Employment contracts and contractor agreements include confidentiality undertakings, intellectual-property assignments, an acknowledgement of and obligation to comply with this Policy, and disciplinary consequences of non-compliance.

15.3 Awareness, Education and Training

All Personnel complete information security awareness training upon onboarding and at least annually thereafter. The training programme covers, at a minimum, this Policy, password and authentication hygiene, phishing and social-engineering recognition, secure handling of player personal data, incident reporting, the responsible-gaming context, and AML/CFT data sensitivities. Personnel in roles with elevated risk receive additional, role-specific training (e.g., secure development, treasury operations, customer-facing dispute handling).

15.4 Disciplinary Process

Breaches of this Policy are addressed through the Company's disciplinary process, with sanctions ranging from formal warnings to dismissal for cause and, where applicable, the pursuit of civil or criminal liability. The application of the disciplinary process is consistent with applicable employment law and with the Code of Conduct.

15.5 Termination and Change of Role

On termination of employment or contract, or on a material change of role, the joiner-mover-leaver process described in Section 8.2 is followed. Departing Personnel are reminded in writing of their continuing obligations of confidentiality and of the prohibition on retaining or using Company information after departure.

16. Information Security Incident Management

16.1 Reporting

All Personnel must report any actual or suspected information security incident — including, without limitation, suspected unauthorised access, malware, phishing, data leak, lost or stolen device, or unusual system behaviour — to Management without undue delay through the channels published in the Incident Response Procedure. Players and external parties may report security concerns through the channels described in the Privacy Policy and the Player Complaints & Dispute Resolution Policy.

16.2 Detection and Triage

Incidents are triaged by a designated incident handler, who: (i) classifies the incident by severity and category; (ii) opens an incident record; (iii) initiates containment measures; and (iv) convenes the Incident Response Team for incidents of moderate or higher severity.

16.3 Containment, Eradication and Recovery

The Incident Response Team takes all reasonable steps to contain the incident, eradicate the underlying cause and recover affected services, while preserving evidence to the extent practicable.

Decisions affecting players (e.g., suspending withdrawals, forced password resets) are taken by Management in consultation with the operational leadership.

16.4 Notifications

Management, where appropriate, external counsel:

- notifies the CGA in accordance with the Company's licence conditions and any applicable CGA reporting requirements;
- notifies the Office for Personal Data Protection of personal data breaches as required by the LBP and, where applicable, by the GDPR (including, for GDPR-covered breaches, within 72 hours of becoming aware of the breach);
- notifies affected Data Subjects where the breach is likely to result in a high risk to their rights and freedoms, in accordance with the LBP and the GDPR;
- notifies law enforcement and other competent authorities where required;
- communicates with players, partners and the public in a manner consistent with regulatory requirements, contractual obligations and the Company's reputation; and
- documents all decisions, notifications and timelines for the regulatory record.

16.5 Post-Incident Review

Every material incident is followed by a documented post-incident review. The review identifies the root cause, the effectiveness of the response, the lessons learned and the corrective actions, with owners and target dates. Management tracks corrective actions through to closure and reports the status to the Board.

17. Compliance, Audit and Review

17.1 Internal Compliance Monitoring

Management performs continuous monitoring of compliance with this Policy and its supporting standards, using key risk and key control indicators. Material findings are escalated to senior management and to the Board.

17.2 Internal Audit

The Company subjects the information security program and the controls described in this Policy to internal audit on a risk-based schedule and at least annually for licence-critical processes. Internal audit operates with appropriate independence from the activities it audits.

17.3 Independent External Audit and Testing

The Company commissions independent external assessments where required by the CGA or where appropriate to the risk, including: (i) external penetration testing of the Platform; (ii) external audits of game integrity and RNG; and (iii) external assurance over relevant portions of the information security program. External findings are tracked in the same way as internal findings.

17.4 Regulatory Cooperation

The Company cooperates fully and in good faith with the CGA, the Office for Personal Data Protection, the Financial Intelligence Unit (FIU) of Curaçao and other competent authorities, including by providing information, granting access to systems and premises (subject to applicable legal protections), and by responding to requests within the timelines specified by the relevant authority. Where lawful, the Company may be restricted from disclosing certain regulatory communications to data subjects or third parties.

17.5 Management Review

Senior management reviews the information security program at least annually, on the basis of a written management report. The review covers: the status of the risk register; the results of audits and tests; significant incidents; the status of corrective actions; the adequacy of resources; and any necessary changes to this Policy and supporting documents. Decisions arising from the review are recorded and tracked.

17.6 Consequences of Non-Compliance

Non-compliance with this Policy may result in: (i) disciplinary action against Personnel up to and including dismissal; (ii) termination of contracts with third parties; (iii) civil claims for damages; (iv) regulatory action by the CGA, the Office for Personal Data Protection or other authorities, including warnings, fines, conditions on, suspension or revocation of the Company's licence; and (v) criminal liability where applicable under Curaçao law.

18. Regulatory and Reference Framework

18.1 Curaçao Legal Framework

- National Ordinance on Games of Chance (Landsverordening op de kansspelen — “LOK”), as amended, and the licensing and operational requirements issued by the CGA;
- National Ordinance on Personal Data Protection (Landsverordening bescherming persoonsgegevens — “LBP”);
- National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties — “LMOT”);
- National Ordinance on the Identification of Service Providers (Landsverordening identificatie bij dienstverlening — “LID”);
- National Ordinance on the Prevention and Combating of Money Laundering and the Financing of Terrorism, and implementing regulations and guidance issued by the CGA and the FIU of Curaçao;
- Civil and Criminal Codes of Curaçao, in respect of confidentiality, fraud, computer crime and related offences.

18.2 Other Applicable Frameworks

- Regulation (EU) 2016/679 (GDPR), where applicable to the processing of personal data of players in the European Union or the European Economic Area;
- Payment Card Industry Data Security Standard (PCI DSS), where applicable to the handling of payment-card data, including through processors;
- Financial Action Task Force (FATF) Recommendations, as implemented through Curaçao law and the Company's AML/CFT Policy.

18.3 Aligned Best Practices

- NIST Cybersecurity Framework and NIST SP 800-series publications;
- OWASP Application Security Verification Standard (ASVS) and Top 10.

18.4 Related Internal Documents

- Privacy Policy (Crypto.Games);
- AML/CFT Policy (MuchGaming B.V.);
- Code of Conduct (Crypto.Games);
- Responsible Gaming Policy (Crypto.Games);
- Self-Exclusion Policy (Crypto.Games);
- Player Complaints & Dispute Resolution Policy (Crypto.Games);
- Operational Manual (Crypto.Games);
- Supporting standards: Acceptable Use Standard, Data Handling Standard, Authentication Standard, Cryptography Standard, Key Management Standard, Logging and Monitoring Standard, Vulnerability Management Standard, Endpoint Security Standard, Incident Response Procedure, Business Continuity and Disaster Recovery Plan, Third-Party Risk Management Procedure.

19. Contact Information

Questions about this Policy, suspected security weaknesses or incidents, and requests from regulators may be directed to:

- Security matters — security@crypto.games
- AML Officer — sportillo@xcm.cw
- General player support — support@crypto.games

MuchGaming B.V., Korpuraalweg 10, Willemstad, Curaçao.

20. Policy History

Version	Date	Approved By	Summary of Change
1.0	May 2026	Board of Directors, MuchGaming B.V.	Initial issue.

21. Policy Owner and Review

This Policy is owned by the Board of Directors and reviewed at least annually, and on every material change to the Company's operations, the threat landscape or applicable law and regulation. Any material amendment requires Board approval.

22. Document URL

This Policy is published internally on the Company's policy portal and a controlled copy is provided to the CGA on request.