

INFORMATION SECURITY POLICY

Teknocode B.V.

Curaçao CoC No.: 171943

Registered office: Dr. M.J. Hugenholtzweg 25, Curaçao

Incorporated: 22 September 2025

Version 2.0 — June 2026

Owner: Statutory Director

Next Review Date: June 2027

1. Purpose

The purpose of this Information Security Policy (this "Policy") is to establish a framework for protecting the confidentiality, integrity and availability of the online gaming platform operated by Teknocode B.V. (the Company) and of the systems, data and services associated with it (collectively, the Platform). This Policy sets out the security principles, controls and mechanisms implemented within the Platform to safeguard user data, financial transactions, system operations and regulatory compliance requirements. It ensures that the security practices adopted by the Company are consistent with licensing and audit expectations under the Curaçao regulatory framework, including in respect of secure authentication, data protection, monitoring and auditability.

This Policy has been prepared having regard to the Curaçao National Ordinance on Games of Chance (Landsverordening op de Kansspelen, the "LOK"), the National Ordinance on Casinos in Curaçao (Landsverordening Casinowezen Curaçao, the "LCC") and the Information Security Control Requirements for CGA Licensees published by the Curaçao Gaming Authority (the "CGA"), and is intended to be construed and applied consistently with the Center for Internet Security Controls Version 8 Implementation Group 1 ("CIS IG1") baseline and, so far as proportionate, with the international information security management standard ISO/IEC 27001:2022.

2. Scope

This Policy applies to all components, users and processes associated with the Platform. In particular, and without limitation, this Policy covers:

- All components of the Online Gaming Platform, including player-facing applications, administrative systems, application programming interfaces (APIs) and backend services.
- All modules, including without limitation authentication, payments, wallet, notifications, content management and affiliate systems.
- All data processed, stored or transmitted within the Platform, including player data, financial transactions, know-your-customer (KYC) documentation and system logs.
- All users interacting with the Platform, whether players, operators or integrated third-party services.
- All persons acting for or on behalf of the Company, whether as officers, employees, contractors, consultants or agents.
- All cloud, managed and outsourced services supporting the operation of the Platform, whether contracted directly by the Company or by an operator counterparty.

The scope of this Policy extends to the security controls implemented across the infrastructure, application and operational layers of the Platform. Where this Policy refers to a control being

applied within the Platform, such reference shall be construed as extending to any functionally equivalent control implemented by a service provider on behalf of the Company.

3. Information Security Principles

The Platform is designed and operated on the basis of four foundational information security principles. Confidentiality requires the protection of sensitive data — including personal information, authentication credentials and financial data — from unauthorised access, disclosure or exposure. Integrity requires the accuracy and consistency of data to be preserved through secure transaction handling and comprehensive audit trails. Availability requires that access to the Platform be continuous and reliable, and be supported by a resilient architecture and by real-time monitoring. Accountability requires that all user and system activities be traceable through comprehensive logging and audit mechanisms.

These principles inform the design, implementation and operation of every control described in this Policy and shall be taken into account by every person acting for or on behalf of the Company in the performance of their duties.

4. Governance, Roles and Responsibilities

Overall accountability for the establishment, maintenance and effectiveness of the information security programme of the Company rests with the Statutory Director. The Statutory Director shall approve, and from time to time review, this Policy and the subordinate procedures and standards to which it refers; shall ensure that adequate financial and human resources are made available for its implementation; and shall consider the outputs of internal reviews, independent assurance activities and regulatory correspondence when directing the security posture of the Company.

Day-to-day operational responsibility for information security is delegated to the Chief Technology Officer of the Company (the “CTO”), acting in the capacity of Security Lead. The CTO shall maintain the asset and data inventories of the Company, coordinate risk assessment, control implementation and control testing, act as principal point of contact for third-party assurance providers and regulators, and prepare an annual information security report for the Statutory Director. Every officer, employee and contractor of the Company is responsible for complying with this Policy in the performance of their duties and for reporting, without undue delay, any actual or suspected Security Incident, control weakness or policy breach.

5. Information Security Management System

The Company operates an Information Security Management System (the “ISMS”) constructed around the plan-do-check-act cycle familiar from ISO/IEC 27001:2022. The ISMS shall comprise, at a minimum, this Policy, the subordinate procedures and technical standards referred to herein, the asset inventory of the Company, its risk register and treatment plan, the record of Security

Incidents and control deficiencies, the record of internal and external assurance activities and the outputs of the annual management review. Risk assessment shall be performed on a continuing basis and formally documented at least annually. Risk acceptance decisions shall in every case be documented and authorised by the Statutory Director.

6. Verification Procedures

The Platform enforces mandatory verification and validation of the security controls implemented within it to ensure their effectiveness and their proper implementation. The verification mechanisms operated by the Company include, without limitation:

- E-mail, phone (OTP) and device verification flows with defined expiry, retry limits and lock-out controls.
- CAPTCHA validation (Cloudflare Turnstile) to prevent automated abuse.
- Rate limiting and brute-force protection on authentication and other sensitive endpoints.
- Transaction validation controls, including the prevention of duplicate transactions through cryptographic hashing.
- Comprehensive logging and audit trails to verify control effectiveness on an ongoing basis.

The verification controls of the Platform are continuously monitored and validated through system-enforced rules, structured logging and audit mechanisms, and are reviewed by the CTO for adequacy and effectiveness at least once per calendar year.

7. Asset Management

The Company manages information assets through structured ownership, classification and handling controls. The platform modules of the Platform operate within a modular architecture with defined service boundaries, and operator and system actions are tracked through audit logs designed to ensure accountability. Information assets within scope include, without limitation, player data (identity, contact and KYC documents), financial data (transactions and wallet balances), authentication data (tokens, passwords and device metadata) and system and audit logs; all such data is treated as sensitive and protected accordingly.

In the handling of information assets, the Company shall apply the following requirements without derogation: sensitive data is encrypted at rest using AES-256; credentials and tokens are hashed using industry-standard functions (including bcrypt, SHA-256 and HMAC) and are not stored in plaintext; access to information is restricted through authentication, session control and role-based permissions; and all data access and modification is logged and remains traceable. Inventories of hardware, software and data assets are maintained by the CTO and are reviewed at least twice per calendar year.

8. Access Control and Authentication Security

The Platform implements strong access control mechanisms designed to prevent unauthorised access to information and to systems. Authentication is effected through a secure login flow employing username and password credentials with optional Time-based One-Time Password (TOTP-based) two-factor authentication. CAPTCHA validation is deployed to prevent automated attacks, and sessions are bound to specific devices by means of unique session tokens. Configurable session timeouts and inactivity controls are enforced, and single active session enforcement is applied to non-test accounts.

Password security shall be maintained through the following controls: passwords shall be hashed at rest using bcrypt with an appropriate cost factor; password reset flows shall be secured through one-time password (OTP) mechanisms with defined expiry and rate limits; and password complexity rules shall be enforced at the point of registration and change. Operator-level access to the Platform shall be governed on the basis of role, shall be subject to full audit tracking and shall be periodically reviewed for continued business necessity.

9. Data Protection and Encryption

The Platform enforces strong encryption standards for the protection of sensitive information. AES-256 encryption is applied to sensitive data at rest, including without limitation KYC documents and payment data. SHA-256 and HMAC hashing are applied to tokens and to secure lookups, and secure key derivation mechanisms are employed where cryptographic keys are generated from user secrets. Encryption of data in transit shall be effected through modern Transport Layer Security (TLS) protocols using strong cipher suites, and legacy protocols such as SSL and early TLS versions shall be disabled.

Additional protections applied within the Platform include the following: no sensitive data shall be stored in plaintext; backup codes shall be subject to one-way hashing so that they cannot be recovered in cleartext; and encryption operations shall employ initialisation vectors (IVs) and authentication tags where required by the underlying algorithm. Cryptographic keys shall be generated, stored, distributed, rotated and destroyed in accordance with the Cryptographic Controls and Key Management section of this Policy.

10. Cryptographic Controls and Key Management

Only algorithms and protocols currently recognised as strong by international standards bodies (including the National Institute of Standards and Technology and the European Union Agency for Cybersecurity) shall be used within the Platform. Deprecated algorithms shall be retired in accordance with the change control procedure. Cryptographic keys shall be generated, stored, distributed, rotated and destroyed in accordance with a documented key-management standard, with high-value keys held in hardware security modules or in equivalent, access-controlled

storage. Data masking shall be employed where personnel require visibility of data structures but do not require access to the underlying sensitive information.

11. Network Security Management

The Platform enforces network security through layered controls. Internal application programming interfaces (APIs) are secured through authentication; the microservice-based architecture of the Platform ensures the isolation of components; and internet-protocol (IP) blocking, virtual private network (VPN) detection and middleware validation are applied at appropriate points in the request flow. Traffic monitoring and threat detection are implemented through full HTTP request logging (including payload, headers and response), VPN detection through Cloudflare and external validation, and rate limiting together with anomaly detection.

Intrusion detection and prevention are effected through middleware-based request validation, automated IP blocking with audit tracking, and cached enforcement of block-lists to support real-time protection. Network segmentation shall be maintained so that production systems are isolated from corporate and development environments and lateral movement is constrained in the event of a compromise. Perimeter and internal firewalls shall be configured on the basis of default-deny rules.

12. Technical Controls and System Hardening

The Company implements technical controls for the secure operation of the Platform. Configuration management shall be centralised, shall permit runtime updates where appropriate and shall expose configurable security settings (sessions, limits, verification thresholds). System hardening shall be effected through enforced authentication flows (including two-factor authentication and device verification), session controls and inactivity timeouts, and brute-force protection together with account lock mechanisms.

Endpoint protection shall include rate limiting on sensitive endpoints, input validation and request monitoring, and secure token handling and expiration. Data protection controls include the encryption of sensitive data, secure hashing of credentials and the prevention of fraud and duplicate transactions. Secure configuration standards for servers, endpoints and network infrastructure shall be documented, reviewed annually and applied consistently across the environment.

13. Application Security Controls

The application layer of the Platform enforces the following controls without derogation: rate limiting on sensitive endpoints, brute-force protection and account lock-outs, duplicate transaction prevention, secure device verification, and input validation together with request monitoring. Secure development practices shall be applied to the design, coding, testing and deployment of

the application, and changes to the application code base shall be subject to peer review, static analysis and, where practicable, dynamic security testing. Penetration testing of the application shall be performed by a competent, independent party at an interval not exceeding twelve months and following any material change to the application.

14. Transaction and Payment Security

Financial operations conducted through the Platform shall be secured through the following controls: secure integration with payment gateways; full life-cycle tracking of transactions from initiation through settlement to reconciliation; internet-protocol (IP) tracking together with fraud-detection mechanisms; and withdrawal-eligibility enforcement to ensure that withdrawals are executed only in accordance with the applicable policies of the operator and the applicable regulatory framework. Financial calculations shall be performed with appropriate numerical precision and shall be protected against concurrency-related errors.

15. Logging, Monitoring and Audit Trails

The Platform maintains comprehensive logging and audit trails to support control effectiveness, incident investigation and regulatory oversight. The logging and monitoring regime includes full request and response logging, exception tracking with deduplication, session and login tracking, and end-to-end audit trails covering financial and operational events. Logs shall be retained for such minimum period as may be prescribed by the CGA and, in any event, for a period of not less than twelve months. Logs shall be protected against unauthorised modification and deletion; their integrity shall be verifiable; and time sources across the estate shall be synchronised using authoritative network time protocol servers to ensure the correlation of events.

16. Data Integrity and System Reliability

Data integrity within the Platform shall be maintained through precision-based financial calculations, appropriate concurrency controls for transactions, the delivery of real-time updates over persistent connections (including through WebSocket protocols where used) and an event-driven architecture that supports auditable, deterministic processing of business events. Reliability shall be supported through resilient service design, defensive coding practices and the incorporation of health monitoring at each layer of the Platform.

17. User Privacy and Data Handling

The Company shall practise minimum-necessary data collection: only such personal and financial data as is required for the operation of the Platform and for compliance with applicable law shall be collected. Personal and financial data shall be encrypted in accordance with the data protection controls of this Policy, and operator access to such data shall be governed on the basis of role,

business necessity and audit-tracked authorisation. Where processing of personal data is performed on behalf of an operator counterparty, such processing shall be governed by a written data processing agreement that reflects the respective roles and responsibilities of the parties.

18. Responsible Gaming and Protection Controls

The Platform supports the operators to whom it is licensed with technical mechanisms designed to enable responsible gaming outcomes at the end-player level. These mechanisms include configurable deposit and betting limits, account suspension and closure functionality, and the monitoring of activity for anomalies indicative of harmful play. The primary regulatory responsibility for the interaction with end players rests with the operator counterparty; the Company shall cooperate with such operators to ensure that responsible-gaming controls are configured, monitored and evolved in a manner consistent with the applicable regulatory framework.

19. Vulnerability and Patch Management

The Company shall operate a vulnerability management programme that identifies, evaluates and remediates known vulnerabilities affecting its assets and its platform. Automated vulnerability scanning shall be performed at least monthly on internal and external-facing systems and shall be complemented by periodic penetration testing performed by a competent, independent party at an interval not exceeding twelve months and following any material change to the environment. Security patches issued by vendors shall be applied within a period commensurate with the severity of the underlying vulnerability, following an appropriate risk assessment.

20. Backup and Recoverability

The Company shall maintain an automated and regularly tested backup regime for all data and systems whose loss would materially prejudice its operations or the fulfilment of its contractual or regulatory obligations. Backups shall be encrypted, held in geographically separated locations and protected against unauthorised access, modification and deletion. Recovery objectives (recovery time objective and recovery point objective) shall be defined for each critical service, and the capability to meet those objectives shall be verified by testing at least annually.

21. Third-Party Risk Management

The Company relies on a defined set of third-party providers (including hosting and infrastructure providers, testing laboratories, banking counterparties, legal advisors and compliance consultants) and, prior to engaging any such provider, shall conduct a written due diligence exercise addressing the provider's corporate standing, regulatory status (where applicable), security posture, sanctions and adverse-media profile, subcontracting practices and financial resilience. Written agreements with critical providers shall address information security

obligations, incident notification, audit rights, service-level commitments, personal data processing and return or destruction of data on termination. A register of critical suppliers shall be maintained by the CTO, together with a documented alternative for each critical category.

22. Physical and Environmental Security

Although the operations of the Company are predominantly conducted through digital channels, the physical environment in which its personnel work and in which its equipment and records are held remains a material control layer. Access to the premises of the Company and to areas in which sensitive information may be viewed or stored shall be restricted to authorised persons. Where the Company relies on data-centre or co-location services provided by a third party, the physical security controls of that provider shall be assessed as part of the third-party due diligence process.

23. Human Resource Security

Personnel security controls shall be applied throughout the employment life-cycle. Background verification checks shall be performed on all personnel proposed to access sensitive information or to occupy positions of trust, in a manner proportionate to the sensitivity of the role and having regard to applicable law. Personnel shall be subject to written confidentiality obligations and to a code of conduct that reflects the requirements of this Policy. Upon the termination of any engagement, access rights shall be revoked and Company property and information shall be returned or securely destroyed.

24. Security Awareness and Training

The Company shall implement and maintain a security awareness and training programme designed to equip personnel to identify, avoid and report information security risks. All personnel shall complete training at induction and at least annually thereafter, with additional targeted training provided to personnel occupying roles with elevated risk profiles. Training records shall be maintained by the CTO and shall be made available to the Statutory Director and, on request, to the CGA.

25. Incident Management and Response

The Company shall maintain a documented Security Incident response procedure providing for the real-time monitoring of anomalies, the logging of all system events, operator intervention capabilities and audit-supported investigations. The procedure shall define escalation paths, decision-making authority, roles and responsibilities during an incident, and communication practices (both internal and external). Regulatory notifications shall be made in accordance with the breach-notification requirements of the CGA and, where applicable, other supervisory or legal

obligations. Post-incident reviews shall be conducted for every material Security Incident and tabletop exercises shall be conducted at least annually.

26. Business Continuity and Operational Resilience

The Company shall maintain a business continuity plan and a disaster recovery plan designed to enable the continuation, or the timely resumption, of its critical activities in the event of a disruption. The plans shall identify the critical business functions of the Company, the resources on which they depend, the recovery objectives applicable to each such function and the sequence and responsibility for their restoration. The plans shall be tested at least annually and shall be reviewed and revised whenever there is a material change to the activities of the Company, its dependencies or the threat environment.

27. Compliance and Audit Readiness

The Company shall be prepared, at all times, for internal reviews and external audits of its information security controls. To that end, complete audit trails shall be maintained; compliance parameters shall be configurable and documented; and data retention and reporting capabilities shall be sufficient to enable the timely production of information required by internal management, external auditors, operator counterparties and the CGA. The Company shall cooperate in good faith with the CGA and with any other competent authority in the exercise of its supervisory and enforcement functions.

28. Continuous Security Controls

The Platform operates continuous security controls designed to adapt to changing threat conditions and to evolving regulatory expectations. Security settings shall be configurable at runtime and shall be reviewed by the CTO on a periodic basis. User behaviour shall be continuously monitored for anomalies indicative of misuse or compromise. Policies shall be enforced consistently across the modules of the Platform, and the outputs of monitoring shall inform ongoing improvements to the security controls of the Company.

29. Policy Review and Continuous Improvement

This Policy shall be reviewed by the Statutory Director at least annually and upon the occurrence of any material change to the activities, information systems, regulatory environment or risk profile of the Company. The outcome of each review, whether resulting in amendment of this Policy or in its readoption without change, shall be documented.

30. Document Control

- Version: 2.0.
- Date of issue: June 2026.
- Owner: Statutory Director (MAX Management and Corporate Services B.V.).
- Next scheduled review: June 2027.
- Supersedes: Information Security Policy, Version 1.0 (September 2025).

31. Adoption and Approval

This Policy is adopted by, and issued under the authority of, the Statutory Director of Teknocode B.V. It supersedes the Information Security Policy, Version 1.0, of September 2025, and enters into force upon signature below.

For and on behalf of Teknocode B.V.



MAX Management and Corporate Services B.V.
Statutory Director

Date: 13 August 2026

Place: Curaçao