

INFORMATION SECURITY AND CYBER RESILIENCE POLICY

*Adopted pursuant to the National Ordinance on Games of Chance (LOK) and the Information Security Control Requirements
of the Curaçao Gaming Authority*

Lord Structure B.V.

Curaçao CoC No.: 168598

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

Incorporated: 17 October 2024

Document Reference:

LS/ISPOL/01-2026

Edition 2026-01

Owner: Statutory Director

Article 1 Preamble and Legal Foundation

The Statutory Director of Lord Structure B.V. (the “Licensor”), being a Curaçao private limited liability company registered with the Curaçao Chamber of Commerce and Industry under number 168598 and engaged in the development, production and licensing of certified online casino game content on a Business-to-Business basis to licensed Business-to-Consumer operator counterparties, hereby resolves to adopt and promulgate this Information Security and Cyber Resilience Policy (the “Policy”). The Policy constitutes the governing instrument by which the Licensor identifies, assesses, treats and monitors information security and cyber-resilience risk in the context of its regulated activities and its dealings with counterparties.

Adoption of the Policy has been undertaken in compliance with, and in furtherance of, the provisions of the National Ordinance on Games of Chance (Landsverordening op de Kansspelen, “LOK”), the National Ordinance on Casinos in Curaçao (Landsverordening Casinowezen Curaçao, “LCC”) and the Information Security Control Requirements for CGA Licensees (the “CGA Requirements”) published by the Curaçao Gaming Authority (the “Authority”). The principles reflected herein are further intended to be interpreted, so far as is reasonably practicable, in a manner consistent with the Center for Internet Security Controls Version 8 Implementation Group 1 (“CIS IG1”) and, where proportionate to the Licensor’s business, with the international information security management standard ISO/IEC 27001:2022.

Save as expressly stated to the contrary, references in the Policy to the “Licensor” shall include the Statutory Director, the Ultimate Beneficial Owner acting in that capacity, and any officer, employee, contractor or agent acting under authority of the Statutory Director. The Policy shall be read together with the subordinate procedures and technical standards to which it refers, and shall bind the Licensor from the date of signature below until it is duly amended or replaced.

Article 2 Interpretation and Defined Terms

In the Policy, save where the context otherwise requires, the terms set out below shall bear the meanings ascribed to them. Terms not so defined shall bear the meaning given to them in the CGA Requirements or, failing that, the meaning commonly attributed to them within the information security profession.

“Critical Gaming Data” shall mean game outcome records, random number generator (“RNG”) output logs, jackpot triggers, wager and settlement records and any other information the integrity of which is material to the fairness or reliability of the games licensed by the Licensor. “Sensitive Information” shall mean, collectively, Critical Gaming Data, Personal Data, Confidential Information and any other information the loss, unauthorised disclosure or unauthorised modification of which would materially prejudice the Licensor or any third party. “Security Incident” shall mean any event

or series of events that compromises, or is reasonably capable of compromising, the confidentiality, integrity or availability of information or information systems within the scope of the Policy.

Article 3 Scope of Application

The following persons, assets and processes fall within the scope of this Policy:

- All information created, received, stored, processed or transmitted by the Licensor, in whatever form or medium.
- All information systems, applications, remote game server elements, source code, integration interfaces and infrastructure operated by or on behalf of the Licensor.
- All cloud, managed and outsourced services supporting the Licensor's activities.
- All officers, employees, contractors, consultants, agents and other natural persons acting for or under the authority of the Licensor.
- All premises and workspaces from which the Licensor's business is conducted.

Article 4 Governance and Allocation of Responsibility

Overall accountability for the Policy and for the information security posture of the Licensor is reserved to the Statutory Director. In the discharge of that accountability, the Statutory Director must approve, and periodically review, this Policy; ensure that adequate financial and human resources are made available for its implementation; and consider the outputs of internal reviews, independent assurance activities and regulatory correspondence when giving direction to the Licensor's security programme.

Operational responsibility for the execution of the Policy is delegated to a Security Lead designated by the Statutory Director. The Security Lead must keep the Licensor's inventories, coordinate risk assessment, control implementation and control testing, act as principal interface with third-party assurance providers and prepare an annual report to the Statutory Director. Every natural person acting for or under the authority of the Licensor must comply with the Policy and must report, without undue delay, any actual or suspected Security Incident, control weakness or policy breach.

Where the Licensor entrusts any material information-processing activity to a third party, such delegation must not derogate from the Licensor's accountability under the Policy in respect of the activity concerned; the arrangement must in every case be governed in accordance with the article dealing with third-party risk management.

Article 5 Information Security Management System

The Licensor operates an Information Security Management System (the “ISMS”) organised around the plan-do-check-act cycle contemplated by ISO/IEC 27001:2022. The ISMS must include, at a minimum, the Policy, its subordinate procedures and standards, the Licensor’s asset inventory, its risk register and treatment plan, its record of Security Incidents and control deficiencies, the record of internal and external assurance activities and the outputs of the annual management review conducted by the Statutory Director.

Risk assessment must be performed on a continuing basis and shall be formally documented at least once in each calendar year. Risk treatment decisions may consist in the mitigation, transfer, avoidance or informed acceptance of a risk; in every case, risk acceptance decisions must be reduced to writing and must be authorised by the Statutory Director.

Article 6 Classification, Handling and Retention of Information

Every item of information handled by the Licensor must be classified as Critical Gaming Data, Personal Data, Confidential Business Information or Public Information. The applicable classification must determine the handling, storage, transmission, sharing, retention and disposal requirements applicable to the information concerned. A central record of the physical and logical locations at which Sensitive Information is stored, processed or transmitted must be maintained and periodically reconciled with the underlying estate.

Access to Sensitive Information must be restricted on the basis of role and business necessity in accordance with the principle of least privilege and must be subject to periodic review. Retention periods must be defined for each classification, having regard to the LOK requirement that gaming transaction records be retained for the minimum period prescribed by the Authority (and, in any event, for not less than five years). Secure disposal must be effected by cryptographic erasure, secure overwriting, degaussing or physical destruction according to the medium concerned.

Article 7 Cryptographic Controls and Key Custody

Sensitive Information must be protected at rest and in transit by cryptographic controls employing algorithms and protocols currently regarded as strong by international standards bodies (including the National Institute of Standards and Technology and the European Union Agency for Cybersecurity). Algorithms superseded by such bodies must be retired in accordance with the Licensor’s change control procedure. Cryptographic keys must be generated, stored, distributed, rotated and destroyed in accordance with a documented key-management standard, with high-value keys held within hardware security modules or in equivalent controlled storage. Where personnel require visibility of data structures but do not require access to the underlying Sensitive Information, data masking must be employed.

Article 8 Asset Register and Software Estate

The Licensor must maintain up-to-date registers of the hardware and software assets used to support its business. The register of hardware assets must record for each entry its identifier, its physical or logical location, the person or function responsible for it, its network approval status, its principal function and (where relevant) its internet-protocol or media-access-control address. The register of software assets must record for each entry the vendor, the product name and version, the date of installation, the associated business function, the number of licences and the vendor support status. Both registers must be reviewed at least twice in each calendar year.

Unauthorised hardware or software identified within the Licensor's environment must be dealt with promptly by way of quarantine, removal or, where duly approved on the basis of a written justification, sanctioned integration. Software that has passed the vendor's end-of-support must be retired, replaced or subjected to documented compensating controls. Assets bearing on the fairness, integrity or availability of the Licensor's games must be treated as priority assets and must be reviewed with particular care.

Article 9 Secure Configuration and System Hardening

Documented secure configuration standards must be developed and maintained for each category of asset in the Licensor's estate, including physical and virtual servers, security appliances, user endpoints, mobile devices and network infrastructure. Recognised industry baselines (including the CIS Benchmarks) must be adopted as the starting point for those standards, which must be reviewed at least annually and upon the deployment of new technology.

Automatic session locking must be enforced on all user devices after a period of inactivity not exceeding fifteen minutes for general systems and two minutes for mobile devices. Host- and endpoint-based firewalls must be deployed and centrally managed on all supported systems, and default-deny configurations must be applied. Administrative access must be effected only through encrypted and authenticated protocols (including SSH, SFTP and HTTPS); insecure protocols including Telnet, HTTP and FTP must be disabled unless retained under a documented exception. Default accounts must be disabled or renamed and their credentials rotated upon deployment.

Article 10 Identity, Access and Privileged Account Management

The Licensor must maintain an inventory of user, administrator and service accounts. Accounts must be provisioned, modified and deprovisioned in accordance with a documented joiner-mover-leaver procedure. The principle of least privilege must apply to every account; privileged access must be granted only on the basis of demonstrable business necessity, must be subject to enhanced logging and must be periodically re-authorised.

Passwords must comply with a documented password standard designed to resist guessing, brute-force and credential-stuffing attacks. Multi-factor authentication must be required for administrative access to production systems, for access to remote game server components and code repositories and for access to cloud consoles, corporate e-mail and file-sharing platforms. Shared or generic accounts must not be used save in exceptional and documented circumstances, in which case compensating controls must be applied and must be reviewed at least quarterly.

Article 11 Vulnerability, Patch and Change Management

The Licensor must operate a vulnerability management programme addressing the identification, evaluation and remediation of known vulnerabilities. Automated scanning must be performed at least monthly, and must be complemented by penetration testing performed by an independent party at an interval not exceeding twelve months and following any material change to the environment. Vendor patches must be applied within a period commensurate with the severity of the underlying vulnerability, following an appropriate risk assessment. Changes to the environment must be governed by a documented change control procedure incorporating peer review, testing and roll-back planning.

Article 12 Logging, Monitoring and Audit

Audit logging must be implemented across the Licensor's material information systems, including operating systems, application platforms, remote game server components, network devices and cloud services. At a minimum, logs must capture successful and failed authentication events, privileged operations, changes to system configuration and access to Sensitive Information. Logs must be retained for the minimum period prescribed by the Authority and, in any event, for not less than twelve months.

Logs must be protected against unauthorised modification and deletion and their integrity must be verifiable. Alerts must be configured for events indicative of malicious or anomalous activity and must be triaged by the Security Lead without undue delay. Time sources across the estate must be synchronised using authoritative network time protocol servers.

Article 13 Malware Defence and Removable Media

Endpoint protection technology capable of detecting and containing malicious software must be deployed on all workstations and servers under the Licensor's control, together with centrally managed updates and configuration. The use of removable media must be restricted to that which is strictly necessary and must be encrypted where used to hold Sensitive Information. Auto-run and auto-play features must be disabled by default.

Article 14 Protection Against Web and E-mail Threats

The Licensor must protect its personnel from web-borne and e-mail-borne threats through appropriate technical controls, including secure e-mail gateway filtering, spam and phishing detection, malicious URL and attachment analysis and implementation of the SPF, DKIM and DMARC protocols in respect of the Licensor's domains. Personnel must be trained under the awareness programme to recognise and report suspected phishing attempts and social engineering.

Article 15 Backup and Recoverability

The Licensor must maintain an automated and periodically tested backup regime for all data and systems the loss of which would materially prejudice its operations. Backups must be encrypted, held in geographically separated locations and protected against unauthorised access, modification and deletion, including through the use of immutable or air-gapped storage where practicable. Recovery time and recovery point objectives must be defined for each critical service and must be validated by testing on at least an annual basis.

Article 16 Network Segmentation and Perimeter Defence

The Licensor's network must be segmented so as to isolate production from corporate and development environments and to constrain lateral movement in the event of a compromise. Perimeter and internal firewalls must be configured on the basis of default-deny rules, and flows between security zones must be documented, approved and periodically reviewed. Remote access must be delivered only through secure channels employing strong authentication. Wireless networks used for corporate purposes must be secured with contemporary encryption protocols and must be separated from any wireless access made available to visitors.

Article 17 Third-Party Risk and Supply Chain

Before engaging any third party which will have access to Sensitive Information or which will perform any material information-processing activity, the Licensor must conduct a written due diligence exercise addressing the third party's corporate standing, regulatory status (where applicable), security posture, sanctions and adverse-media profile, subcontracting practices and financial resilience. The outputs of the exercise must be documented and revisited at appropriate intervals.

Written agreements with critical third parties must address, as a minimum, information security obligations, incident notification, subcontracting, audit and inspection rights, service-level commitments, personal data processing (where applicable) and return or destruction of data on termination. A register of critical suppliers must be maintained together with a documented alternative for each critical category.

Article 22 Business Continuity and Operational Resilience

The Licensor must 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 must identify the Licensor's critical business functions, the resources on which they depend, the recovery objectives applicable to each function and the sequence and responsibility for their restoration. The plans must be tested at least annually and must be reviewed and revised upon any material change to the Licensor's activities, its dependencies or the threat environment.

Article 23 Legal and Regulatory Compliance

The Licensor must identify, document and comply with the legal, regulatory and contractual requirements applicable to its handling of information and to its use of information systems, including the LOK, the LCC and the guidance issued by the Authority in respect thereof. Where activities of the Licensor involve the processing of Personal Data, such processing must be conducted in accordance with applicable data-protection law. The Licensor must cooperate in good faith with the Authority and any other competent authority in the exercise of its supervisory and enforcement functions.

Article 24 Review, Amendment and Continuous Improvement

The Policy must be reviewed by the Statutory Director at least once in each calendar year and upon the occurrence of any material change to the Licensor's activities, information systems, regulatory environment or risk profile. The outcome of each review, whether resulting in amendment or in readoption without change, must be documented. Subordinate procedures, standards and guidelines must be updated on the same cadence, and material changes must be communicated to personnel and to those third parties for whom knowledge of the change is relevant.

Article 25 Enforcement

Non-compliance with the Policy may result in disciplinary action in accordance with applicable law and the terms of the engagement of the person concerned, up to and including the termination of employment or of the contractual relationship. In cases involving suspected criminal conduct, the Licensor reserves the right to refer the matter to the competent authorities and to cooperate with any subsequent investigation. Nothing in this Article must limit the rights of the Licensor at law or in equity.

Article 26 Adoption

The Policy is hereby adopted by the Statutory Director of the Licensors. It supersedes any prior information security policy of the Licensors (whether written or unwritten) and must enter into force upon signature below.

For and on behalf of Lord Structure B.V.



MAX Management and Corporate Services B.V.
Statutory Director

Date: 13 August 2026

Place: Curaçao