

Information Security Policy

A Framework of Technical, Organisational and Administrative Controls

Ninja Technologies B.V.

Curaçao CoC No.: 170874

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

Incorporated: 11 June 2025

Document Reference:

NT-InfoSec-2026-01

v.1.0 / 2026

Owner: Statutory Director

Chapter I Purpose and Legal Basis

This Information Security Policy sets out the operational framework within which Ninja Technologies B.V. (the Provider, a Curaçao private limited liability company registered under number 170874 and engaged in the development, licensing and supply of certified online casino game content, on a Business-to-Business basis, to licensed Business-to-Consumer operators) will protect the confidentiality, integrity and availability of the information assets, technology environments and counterparty data entrusted to it. It defines the roles and control expectations that apply across the Provider's activities, and it functions as the parent document for the technical and procedural standards operated by the Provider's Security Function.

The regulatory obligations of the Provider arise principally under the Curaçao National Ordinance on Games of Chance (LOK) and the Information Security Control Requirements published by the Curaçao Gaming Authority (the "CGA"). Those obligations are given effect through the present Policy. The technical controls referred to herein have been aligned with the Center for Internet Security Controls Version 8 Implementation Group 1 ("CIS IG1"), with wider alignment to ISO/IEC 27001:2022 to be pursued on a progressive basis consistent with the CGA's cybersecurity maturity roadmap.

Chapter II Scope and Application

This Policy is applicable to the following, without limitation:

- All information created, received, stored, processed or transmitted by the Provider, whether in electronic or physical form.
- All information systems, applications, remote game server components, code repositories, integration endpoints, workstations, mobile devices and network infrastructure operated by or on behalf of the Provider.
- All cloud, managed and outsourced services supporting the activities of the Provider.
- All officers, employees, contractors, consultants, agents and other individuals acting for or on behalf of the Provider.
- All premises, meeting spaces and workspaces from which the Provider's business is conducted, wherever located.

The Policy will apply irrespective of the geographical location of the person, asset or activity concerned, and will be read together with the subordinate procedures, technical standards and guidelines to which it refers.

Chapter III Governance, Roles and Responsibilities

Overall accountability for the establishment, maintenance and effectiveness of the information security programme of the Provider rests with the Statutory Director. The Statutory Director will approve, and from time to time review, this Policy and any subordinate procedures, will ensure that adequate financial and human resources are made available for its implementation, and will take into account the outputs of internal reviews, independent assurance activities and regulatory correspondence when directing the security posture of the Provider.

Day-to-day operational responsibility for the execution of this Policy is delegated to a suitably qualified individual designated by the Statutory Director (the “Security Lead”). The Security Lead will maintain the inventories referred to in the Policy, coordinate risk assessment, control implementation and control testing, act as principal point of contact for third-party assurance providers and prepare an annual information security report for the Statutory Director. Every officer, employee and contractor of the Provider 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.

Chapter IV Information Security Management System

The Provider operates an Information Security Management System (the “ISMS”) constructed around the plan-do-check-act cycle familiar from ISO/IEC 27001:2022. The ISMS will comprise, at a minimum, this Policy, the subordinate procedures and technical standards referred to herein, the asset inventory, the 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 will be conducted on a continuing basis and formally documented at least annually. Risk treatment decisions may consist in the mitigation, transfer, avoidance or informed acceptance of a risk; risk acceptance decisions will in every case be documented and authorised by the Statutory Director.

Chapter V Asset Management and Inventory

The Provider will maintain complete and accurate inventories of the hardware and software assets used to support its activities. The inventory of hardware assets will record, in respect of each asset, its identifier, its location (whether physical or logical), the person or business function responsible for it, its network approval status, its principal function and, where relevant, its internet protocol or media access control address. The inventory of software assets will record 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 inventories will be reviewed at least twice each calendar year and after any material change to the estate.

Unauthorised hardware or software identified within the environment of the Provider will be dealt with promptly. The Provider will implement documented procedures for the detection, quarantine, removal or, where justified and duly approved, sanctioned integration of previously unauthorised assets. Software

found to have passed end-of-support will be retired, replaced or subject to documented compensating controls.

Chapter VI Data Classification, Handling and Retention

All information handled by the Provider will be classified as Critical Gaming Data, Personal Data, Business Confidential Information or Public Information. The classification will determine the handling, storage, transmission, sharing, retention and disposal requirements applicable to it. A central record of the physical and logical locations at which Sensitive Information is stored, processed or transmitted will be maintained. Access will be restricted on the basis of role and business necessity in accordance with the principle of least privilege.

Retention periods will be defined for each data category, having regard to the LOK requirement that gaming transaction records be retained for the minimum period prescribed by the CGA (and, in any event, for a minimum of five years unless a longer period is specified). Secure disposal will be effected by cryptographic erasure, secure overwriting, degaussing or physical destruction as appropriate to the medium. Sensitive Information on end-user devices will be protected by full-disk encryption; data in transit will be protected using cryptographically strong protocols as described in the Cryptographic Controls section.

Chapter VII Secure Configuration of Systems and Endpoints

The Provider will develop and maintain documented secure configuration standards for each category of asset used in its environment. Vendor- recommended hardening templates and recognised industry baselines (including the CIS Benchmarks) will be used as the starting point for such standards, which will be reviewed at least annually and upon deployment of any new technology.

Automatic session locking will 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-based firewalls will be deployed and centrally managed on all supported servers, and endpoint firewalls with default-deny rules will be applied to workstations. Administrative interfaces will be accessed only by means of encrypted and authenticated protocols such as SSH, SFTP and HTTPS; insecure protocols including Telnet, HTTP and FTP will be disabled unless retained under a documented and risk-justified exception. Default accounts on all systems, applications and devices will be disabled or renamed and their credentials will be rotated to strong, unique passwords upon deployment.

Chapter VIII Access Control and Identity Management

The Provider will maintain an inventory of user, administrator and service accounts across its systems. Accounts will be provisioned, modified and deprovisioned on the basis of a documented joiner-mover-

leaver procedure. The principle of least privilege will apply to every account; privileged access will be granted only on the basis of demonstrable business necessity and will be subject to enhanced logging and periodic re-authorisation.

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

Chapter IX Vulnerability and Patch Management

The Provider will operate a vulnerability management programme that identifies, evaluates and remediates known vulnerabilities affecting its assets. Automated vulnerability scanning will be performed at least monthly on internal and, where applicable, external-facing systems, and will be complemented by 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 will be applied within a period commensurate with the severity of the underlying vulnerability, following an appropriate risk assessment.

Chapter X Logging, Monitoring and Audit Trails

The Provider will implement audit logging across its material information systems. Logs will capture, at a minimum, successful and failed authentication events, privileged operations, changes to system configuration and access to Sensitive Information. Logs will 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 will be protected against unauthorised modification and deletion, and their integrity will be verifiable. Alerts will be configured for events indicative of malicious or anomalous activity and will be triaged by the Security Lead without undue delay. Time sources will be synchronised using authoritative network time protocol servers.

Chapter XI Malware Defence and Removable Media

Endpoint protection technology capable of detecting and containing malicious software will be deployed on all workstations and servers, together with centrally managed updates and configuration. The use of removable media will be restricted to that which is strictly necessary, will be encrypted where used to hold Sensitive Information and will be subject to a documented approval procedure. Auto-run and auto-play features will be disabled by default.

Chapter XII Web and E-mail Threat Protection

The Provider will 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 Company's domains. Personnel will be trained under the awareness programme to recognise and report suspected phishing attempts and social-engineering approaches.

Chapter XIII Data Backup and Recoverability

The Provider will 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 and regulatory obligations. Backups will be encrypted, held in geographically separated locations and protected against unauthorised access, modification and deletion. Recovery objectives will be defined for each critical service, and the capability to meet those objectives will be verified by testing on at least an annual basis.

Chapter XIV Network Security Architecture

The network of the Provider will be logically segmented in order to isolate production systems from corporate and development environments and to constrain lateral movement in the event of a compromise. Perimeter and internal firewalls will be configured on the basis of default-deny rules, and all inbound and outbound flows between security zones will be documented, approved and periodically reviewed. Remote access will be provided only through secure channels employing strong authentication. Wireless networks used for corporate purposes will be secured with contemporary encryption protocols and separated from any wireless access provided to visitors.

Chapter XV Cryptographic Controls and Key Management

Cryptographic controls will be applied to Sensitive Information at rest and in transit. Only algorithms and protocols currently recognised as strong by international standards bodies will be permitted; deprecated algorithms will be retired in accordance with the change control procedure. Cryptographic keys will 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 equivalent controlled storage. Data masking will be employed where personnel require access to data structures but do not require access to the underlying Sensitive Information.

Chapter XVI Third-Party Risk Management

The Provider relies on a defined set of third-party providers. Prior to engaging a third party which will have access to Sensitive Information or which will perform any material information-processing activity, the Provider will 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 due diligence exercise will be documented and will be revisited at appropriate intervals thereafter.

Written agreements with critical third parties will 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 will be maintained together with a documented alternative for each critical category.

Chapter XVII Physical and Environmental Security

Although the operations of the Provider are predominantly conducted through digital channels, the physical environment remains a material control layer. Access to the premises of the Provider and to areas in which Sensitive Information may be viewed or stored will be restricted to authorised persons and will be monitored by appropriate means. Where the Provider relies on data-centre or co-location services provided by a third party, the physical security controls of that provider will be assessed as part of the third-party due diligence process.

Chapter XVIII Human Resource Security

Personnel security controls will be applied throughout the employment life-cycle. Background verification checks will 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 will 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 will be revoked and property and information will be returned or securely destroyed.

Chapter XIX Security Awareness and Training

The Provider will implement and maintain a security awareness and training programme designed to equip personnel to identify, avoid and report information security risks. All personnel will complete training at induction and at least annually thereafter, with additional targeted training provided to personnel occupying roles with elevated risk profiles. Training records will be maintained by the Security Lead.

Chapter XX Security Incident Management

The Provider will maintain a documented Security Incident response procedure setting out the identification, classification, containment, eradication, recovery and post-incident review of Security Incidents. The procedure will define escalation paths, decision-making authority, roles and responsibilities during an incident, communication practices and evidence-preservation requirements. Regulatory notifications will be made in accordance with the CGA's breach-notification requirements.

Post-incident reviews will be conducted for every material Security Incident. The outputs will be documented and tabled with the Statutory Director. Tabletop exercises simulating plausible incident scenarios will be conducted at least annually.

Chapter XXI Business Continuity and Operational Resilience

The Provider will 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 will identify the 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 will be tested at least annually.

Chapter XXII Legal and Regulatory Compliance

The Provider will 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 CGA in respect thereof. Where activities involve the processing of Personal Data, such processing will be conducted in accordance with applicable data-protection law.

Chapter XXIII Policy Review and Continuous Improvement

This Policy will 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 Provider. The outcome of each review will be documented. Subordinate procedures, standards and guidelines will be updated in accordance with the same cadence.

Chapter XXIV Enforcement and Sanctions

Non-compliance with this 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 Provider reserves the right to refer the matter to the competent authorities and to cooperate with any subsequent investigation.

Chapter XXV Adoption and Approval

This Policy is adopted by, and issued under the authority of, the Statutory Director of the Provider. It supersedes any previous information security policy of the Provider (whether written or unwritten) and will enter into force upon signature below.

For and on behalf of Ninja Technologies B.V.



MAX Management and Corporate Services B.V.
Statutory Director

Date: 13 August 2026

Place: Curaçao

