

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

INFORMATION SECURITY POLICY
KING ENTERPRISES N.V.

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

POLICY OWNER: KING ENTERPRISES N.V.

APPROVER: CHARLES N. PORTER

DOCUMENT ID / VERSION: KE-IS-02 / 1.1

REVIEW FREQUENCY: ANNUALLY AND UPON MATERIAL CHANGE

NEXT REVIEW DATE: MAY 10, 2027

SECURITY CLASSIFICATION: CONFIDENTIAL

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

TABLE OF CONTENTS

1. COMMITMENT TO INFORMATION SECURITY5

2. SCOPE AND PURPOSE.....5

3. LEGAL AND REGULATORY FRAMEWORK.....6

4. INFORMATION SECURITY PRINCIPLES AND DEFINITIONS.....6

 4.1 Core Security Principles.....6

 4.2 Definitions.....7

5. SECURITY GOVERNANCE AND RESPONSIBILITIES.....8

 5.1 Managing Director and Senior Management.....8

 5.2 Compliance Officer.....8

 5.3 Designated Information Security Function.....8

 5.4 IT, Technical Administrators, and Service Providers.....8

 5.5 Employees, Contractors, and Other Users.....8

6. INFORMATION SECURITY RISK MANAGEMENT.....8

7. HARDWARE, SOFTWARE, AND INFORMATION ASSET MANAGEMENT.....9

 7.1 Enterprise Device Inventory.....9

 7.2 Unauthorized Devices.....9

 7.3 Software Inventory and Support Status.....9

8. DATA CLASSIFICATION, HANDLING, RETENTION, AND DISPOSAL.....10

 8.1 Data Classification.....10

 8.2 Handling and Storage.....10

 8.3 Access to Sensitive Data.....11

 8.4 Retention and Secure Disposal.....11

 8.5 Confidential Regulatory and AML Information.....11

9. SECURE CONFIGURATION, ENDPOINT, WEB, AND EMAIL SECURITY.....11

 9.1 Secure Configuration Standards.....11

 9.2 Session Locking.....12

 9.3 Firewalls and Secure Protocols.....12

 9.4 Default Accounts and Settings.....12

 9.5 Browsers, Email, DNS Filtering, and Anti-Malware.....12

 9.6 Removable Media.....12

10. ACCOUNT, ACCESS, AND AUTHENTICATION MANAGEMENT.....13

 10.1 Account Inventory and Lifecycle.....13

 10.2 Passwords and Authentication.....13

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

10.3 Dormant Accounts.....13

10.4 Privileged Accounts and Separation of Duties.....13

10.5 Multi-Factor Authentication.....13

11. VULNERABILITY AND PATCH MANAGEMENT.....14

11.1 Vulnerability Management.....14

11.2 Patch Management.....14

12. LOGGING, MONITORING, AND AUDIT TRAILS.....14

12.1 Log Management.....15

12.2 Gaming and Regulatory Events.....15

13. NETWORK AND INFRASTRUCTURE SECURITY.....15

14. CRYPTOGRAPHIC CONTROLS AND DATA MASKING.....16

15. BACKUP, RECOVERY, BUSINESS CONTINUITY, AND OPERATIONAL RESILIENCE.....16

15.1 Backup and Recovery.....16

15.2 Business Continuity and Operational Assurance.....17

16. THIRD-PARTY, CLOUD, AND B2B PROVIDER SECURITY.....17

16.1 Regulatory Accountability and Shared Responsibility.....17

16.2 Provider Inventory and Due Diligence.....17

16.3 Contractual Security Requirements.....18

16.4 Certified B2B Providers and Game Content.....18

16.5 Externally Supplied Data and Feeds.....18

17. SECURITY INCIDENT MANAGEMENT AND CGA NOTIFICATION.....18

17.1 Incident Response Roles and Contacts.....18

17.2 Reporting and Response Process.....18

17.3 Mandatory CGA Notification.....19

18. PHYSICAL AND HUMAN RESOURCE SECURITY.....19

18.1 Physical and Environmental Security.....19

18.2 Human Resource Security.....19

19. SECURITY AWARENESS AND ROLE-BASED TRAINING.....20

20. COMPLIANCE MONITORING, AUDIT, REVIEW, AND EXCEPTIONS.....20

20.1 Compliance Evidence and Self-Assessment.....20

20.2 Independent Security Audit.....20

20.3 Policy Review and Continuous Improvement.....21

20.4 Policy Exceptions.....21

21. ENFORCEMENT AND NON-COMPLIANCE.....21

APPENDIX A - MINIMUM CONTROL FREQUENCIES.....22

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

APPENDIX B - DATA CLASSIFICATION AND HANDLING SUMMARY.....23

APPENDIX C - REPORTABLE SECURITY INCIDENT CRITERIA.....24

APPROVAL AND SIGNATURE.....24

1. COMMITMENT TO INFORMATION SECURITY

King Enterprises N.V. (the "Company") is committed to maintaining a secure, controlled, reliable, and auditable gaming environment. The Company shall protect the confidentiality, integrity, and availability of its information, systems, services, and regulated records, including player personal and financial data, gaming and transaction records, Responsible Gaming information, KYC/CDD and AML records, complaints information, security logs, and regulatory reporting data.

As outlined in this Information Security Policy (the "Policy"), the Company shall maintain risk-based technical, organizational, physical, and contractual safeguards designed to prevent unauthorized access, misuse, alteration, disclosure, destruction, fraud, manipulation, and disruption. Information security shall be integrated into governance, operations, third-party oversight, business continuity, incident response, and regulatory compliance.

The Company shall implement the mandatory foundational controls established by the CGA for licensees, based on the Center for Internet Security Controls Implementation Group 1 ("CIS IG1"), within the applicable regulatory implementation period. Progression toward higher cybersecurity maturity, including relevant CIS IG2 controls, shall be considered on a risk-based basis as the Company's systems, services, and threat exposure evolve.

2. SCOPE AND PURPOSE

This Policy applies to all directors, officers, employees, temporary personnel, contractors, consultants, affiliates, and third parties acting for or on behalf of the Company who access, administer, process, store, transmit, support, or otherwise interact with Company information or systems.

This Policy applies to information and technology used in connection with the Company's licensed gaming operations, including, where applicable:

- Gaming platforms, websites, domains, mobile applications, player account systems, and administrative portals;
- Player registration, KYC/CDD, AML/CTF, transaction monitoring, sanctions and PEP screening, Responsible Gaming, complaints handling, fraud prevention, security, and compliance systems;
- Servers, endpoints, network devices, cloud services, hosted infrastructure, databases, backup repositories, communication tools, and security systems;
- Player personal data, financial information, payment information, gaming records, transaction data, source of funds and source of wealth information, complaints evidence, Responsible Gaming records, and regulatory reports;

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

- Systems, services, data feeds, APIs, software components, and infrastructure supplied or operated by B2B providers, hosting providers, payment processors, game providers, and other service providers; and
- Paper records, removable media, physical equipment, and off-premises assets used for Company business.

The purpose of this Policy is to establish the Company's minimum information security requirements, assign responsibilities, define mandatory control outcomes, support regulatory supervision, and ensure that information security risks are identified, assessed, managed, monitored, and remediated. The controls described in this Policy shall be implemented directly by the Company or through relevant service providers according to the Company's operating model and documented allocation of responsibilities. Supporting procedures, inventories, standards, records, and technical evidence may be maintained separately and shall be established, updated, and produced as required. This Policy does not replace any technical assessment, independent audit, configuration review, or validation required by the CGA.

3. LEGAL AND REGULATORY FRAMEWORK

This Policy is established in accordance with the laws, regulations, licensing conditions, contractual obligations, and regulatory guidance applicable to the Company, including:

- The Landsverordening op de Kansspelen ("LOK");
- The Landsverordening Casinowezen Curaçao ("LCC"), where applicable;
- The CGA Information Security Control Requirements for CGA Licensees (B2C and B2B);
- Applicable CGA guidelines, directives, reporting requirements, inspections, and technical validation requirements;
- Applicable privacy, data protection, AML/CTF, recordkeeping, intellectual property, employment, and contractual obligations;
- CIS Controls Implementation Group 1, as adopted by the CGA as the mandatory foundational security baseline; and
- ISO/IEC 27001:2022 principles and controls where referenced by the CGA or otherwise appropriate.

Where this Policy uses the terms "must" or "shall," the requirement is mandatory. Risk-based or proportionate implementation shall be permitted only where the applicable CGA requirement expressly allows it and the rationale, risk assessment, and compensating controls are documented.

4. INFORMATION SECURITY PRINCIPLES AND DEFINITIONS

4.1 CORE SECURITY PRINCIPLES

The Company shall apply the following principles throughout the information lifecycle:

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

- Confidentiality: Information is accessible only to authorized persons, systems, and service providers with a legitimate business, legal, or regulatory need.
- Integrity: Information, game outcomes, transactions, configurations, logs, and regulatory records are protected against unauthorized or improper alteration.
- Availability: Critical systems, information, and services remain available or recoverable within defined operational and regulatory requirements.
- Least Privilege: Access is limited to the minimum permissions required for an approved role or task.
- Need-to-Know: Sensitive information is disclosed only where necessary for authorized responsibilities.
- Defense in Depth: Multiple preventive, detective, and corrective controls are used to reduce single points of failure.
- Accountability and Auditability: Security-relevant actions are attributable, logged, retained, and reviewable.
- Secure by Default: Systems and accounts shall be configured to deny unnecessary access and services unless specifically approved.
- Shared Responsibility: Security responsibilities involving cloud, hosted, or B2B services shall be allocated and monitored without transferring the Company's regulatory accountability.

4.2 DEFINITIONS

Critical Gaming Data: Information that may affect gaming integrity, game outcomes, transaction records, player balances, payout validation, RNG-related records, live data feeds, or regulatory reporting.

Player Data: Information relating to an identified or identifiable player, including identity, financial, behavioral, gaming, transaction, preference, KYC/CDD, AML, complaints, and Responsible Gaming information.

Regulated Data: Information subject to specific protection, retention, access, or reporting requirements under the LOK, CGA requirements, AML/CTF rules, or other applicable obligations.

Sensitive Data: Information requiring protection because unauthorized access, disclosure, alteration, or loss could harm players, the Company, gaming integrity, or regulatory compliance.

Security Incident: An actual or suspected event that compromises or may compromise confidentiality, integrity, availability, gaming integrity, player funds, personal data, regulatory reporting, system availability, or game fairness.

Privileged Account: An account with administrative, security, configuration, system-level, or elevated access rights.

Service Provider: An external entity providing technical, hosting, platform, payment, game, security, data, operational, or professional services to or for the Company.

Material Service Provider: A Service Provider whose systems, services, data, access, certifications, or failure may materially affect licensed operations, gaming integrity, player funds, Regulated Data, critical availability, or regulatory compliance.

Control Owner: The internal role or function accountable for implementing, monitoring, evidencing, reviewing, and remediating an assigned information security control.

5. SECURITY GOVERNANCE AND RESPONSIBILITIES

5.1 MANAGING DIRECTOR AND SENIOR MANAGEMENT

The Managing Director and senior management shall retain executive responsibility for the effectiveness, resources, oversight, and regulatory compliance of the information security program. They shall approve this Policy, support risk treatment and remediation, review significant incidents and material risks, and ensure that security considerations are integrated into business decisions.

5.2 COMPLIANCE OFFICER

The Compliance Officer shall coordinate the regulatory aspects of information security, including CGA communications, incident notification, preservation of regulatory records, alignment with AML/KYC, Responsible Gaming and complaints requirements, and monitoring of legal and licensing obligations. The Compliance Officer shall participate in the review of material security risks, incidents, exceptions, and third-party concerns.

5.3 DESIGNATED INFORMATION SECURITY FUNCTION

The Company shall designate an individual, internal function, or appropriately contracted service with responsibility for coordinating information security activities. This function shall have sufficient authority and access to information to oversee, directly or through documented provider arrangements, security controls, risk assessments, asset and account governance, vulnerability remediation, logging, incident response, third-party security oversight, and security awareness. A primary and backup incident response coordinator shall be designated and their contact information shall be maintained.

5.4 IT, TECHNICAL ADMINISTRATORS, AND SERVICE PROVIDERS

Personnel and service providers responsible for technology shall implement and maintain controls within their assigned scope, apply secure configurations, manage access, maintain required records and inventories, patch systems, protect logs and backups, respond to alerts, and provide evidence of compliance when requested. Technical responsibilities delegated to a provider shall be documented, contractually supported where appropriate, and subject to Company oversight and monitoring.

5.5 EMPLOYEES, CONTRACTORS, AND OTHER USERS

All users shall comply with this Policy, protect credentials and Company assets, use only authorized systems and software, complete required training, report suspected incidents

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

promptly, and maintain confidentiality. Users shall not bypass, disable, or interfere with security controls.

6. INFORMATION SECURITY RISK MANAGEMENT

The Company shall maintain a documented, risk-based process to identify, assess, treat, monitor, and review information security risks affecting gaming systems, player data, financial information, critical services, third-party dependencies, and regulatory obligations.

Information security risk assessments shall be performed at least annually and when material changes occur, including the introduction of new systems, providers, products, payment methods, integrations, infrastructure, remote access methods, or significant operational processes. The assessment shall consider threat likelihood, vulnerability, business impact, player impact, gaming integrity, regulatory consequences, and service continuity.

Risk treatment may include remediation, avoidance, transfer, acceptance, or compensating controls. Acceptance of material residual risk shall require documented management approval and shall not be used to avoid mandatory CGA requirements. Corrective actions shall be assigned, prioritized, monitored, and documented through completion.

Security controls shall be implemented so that they do not unnecessarily compromise game fairness, platform reliability, transaction processing, player experience, or regulatory reporting. Where a control may materially affect performance or availability, the Company shall document the risk assessment, testing, approval, and any compensating safeguards.

7. HARDWARE, SOFTWARE, AND INFORMATION ASSET MANAGEMENT

7.1 ENTERPRISE DEVICE INVENTORY

The Company shall ensure, directly or through relevant service providers, that a complete and accurate inventory is maintained for enterprise devices that access, process, store, transmit, or support Company or gaming information. The inventory shall include, where applicable, servers, network devices, firewalls, endpoints, laptops, mobile devices, security appliances, and other connected equipment within the applicable responsibility scope.

For devices within the applicable responsibility scope, inventory records shall contain sufficient identifying and ownership information, including the device identifier or hostname, IP or MAC address where applicable, asset owner or responsible function, and access or approval status. The Company shall ensure that a formal review is performed at least twice annually and upon significant infrastructure changes, using internal records, provider records, or both.

7.2 UNAUTHORIZED DEVICES

The Company shall ensure that a documented weekly process, using automated discovery, provider reporting, or manual verification as appropriate, is maintained to identify unauthorized, unmanaged, or rogue devices within the applicable environment. Unauthorized devices shall be

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

removed, blocked, quarantined, or otherwise contained. Detection and response actions, exceptions, and justifications shall be recorded.

7.3 SOFTWARE INVENTORY AND SUPPORT STATUS

The Company shall ensure, directly or through relevant service providers, that an inventory of authorized software is maintained for the enterprise environment, including operating systems, gaming and player management applications, security tools, administrative applications, reporting systems, and relevant integrations. Inventory records shall identify the software name, version, purpose, owner or responsible function, and support status where applicable.

Software inventory records shall be reviewed and updated at least twice annually. Vendor support status shall be verified at least monthly through internal review, provider assurance, or both. Unsupported or end-of-life software shall be removed, replaced, isolated, or subject to a documented exception with risk acceptance and compensating controls.

8. DATA CLASSIFICATION, HANDLING, RETENTION, AND DISPOSAL

8.1 DATA CLASSIFICATION

Information categories describe the nature of the information, while classification levels determine the required handling. The approved classification levels are Restricted, Confidential, Internal, and Public, as summarized in Appendix B. The Company shall classify information according to sensitivity, regulatory importance, operational criticality, and potential impact. At minimum, the following categories shall be used:

- Critical Gaming and Regulatory Data: game and transaction records, player balances, payout data, gaming integrity records, regulatory reporting data, FIU-related information, audit logs, and other information essential to regulated operations;
- Player Personal and Financial Data: identity documents, contact information, payment data, KYC/CDD information, SOF/SOW information, account and device data, gameplay and behavioral data, complaints records, Responsible Gaming information, and sanctions or PEP screening results;
- Business Confidential Information: internal financials, contracts, strategies, security information, credentials, configurations, investigations, and operational plans;
- Internal Information: non-public operational information intended for authorized internal use; and
- Public Information: approved website, marketing, regulatory, and communications content intended for public disclosure.

8.2 HANDLING AND STORAGE

Handling requirements shall be proportionate to the classification and shall include approved storage locations, access restrictions, secure transmission methods, sharing limitations, backup

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

requirements, and disposal methods. Sensitive and regulated information shall not be stored in unauthorized personal accounts, unapproved cloud services, or unmanaged devices.

The Company shall ensure that up-to-date documentation is maintained for the principal physical and logical locations where sensitive and regulated information is stored, processed, or transmitted, including on-premise systems, hosted environments, cloud services, shared drives, databases, and backup repositories. Such documentation may be maintained through internal records, contractual schedules, architecture documentation, provider records, or a combination thereof, and shall be reviewed at least annually and upon significant changes.

8.3 ACCESS TO SENSITIVE DATA

Access to sensitive and regulated data shall be restricted through role-based access controls, least privilege, and need-to-know principles. Access shall be reviewed regularly and removed promptly when no longer required. Access by third parties shall be limited, approved, monitored, and governed by contractual confidentiality and security obligations.

8.4 RETENTION AND SECURE DISPOSAL

The Company shall define and enforce retention periods for each category of information based on legal, regulatory, contractual, audit, investigation, and operational requirements. Regulated gaming, transaction, KYC/CDD, AML, complaints, and related compliance records shall be retained for at least five (5) years where required by the Company's regulatory framework or for such longer period as may be required by law, an ongoing investigation, litigation hold, CGA instruction, or competent authority.

Information shall be securely disposed of when retention is no longer required. Approved disposal methods may include cryptographic erasure, secure overwriting, degaussing, certified physical destruction, or secure deletion appropriate to the media and data classification. Disposal shall be documented where the information is sensitive, regulated, or material.

8.5 CONFIDENTIAL REGULATORY AND AML INFORMATION

Access to FIU reports, unusual or suspicious transaction reviews, sanctions investigations, security investigations, and other restricted regulatory information shall be limited to authorized personnel with a legitimate need to know. The Company and its personnel shall comply with applicable non-disclosure and anti-tipping-off obligations.

9. SECURE CONFIGURATION, ENDPOINT, WEB, AND EMAIL SECURITY

9.1 SECURE CONFIGURATION STANDARDS

The Company shall establish, or require relevant service providers to maintain, secure configuration standards for servers, endpoints, network devices, security appliances, cloud

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

resources, applications, and other relevant systems within their respective responsibility scopes. Standards shall use vendor guidance, recognized security baselines, or CIS Benchmarks where applicable and shall be reviewed at least annually or when new technologies are introduced. Changes to security-sensitive configurations shall be authorized, tested where appropriate, documented, and auditable. Exceptions shall require a documented risk assessment, approval, expiry or review date, and compensating controls.

9.2 SESSION LOCKING

General user systems administered by the Company shall automatically lock after no more than fifteen (15) minutes of inactivity. Mobile devices administered by the Company and used to access Company or regulated information shall automatically lock after no more than two (2) minutes of inactivity. For provider-managed systems, the Company shall require or verify equivalent risk-appropriate session controls. Any operational exception shall be documented, risk-assessed, and approved.

9.3 FIREWALLS AND SECURE PROTOCOLS

Within systems and infrastructure under its responsibility, the Company shall ensure that host-based and network firewall controls are enabled and managed on supported systems. Firewall rules shall follow a default-deny or least-access approach, permit only authorized services, and be reviewed, approved, and documented. Administrative and data transfer activities shall use encrypted and authenticated protocols such as SSH, SFTP, and HTTPS. Insecure protocols such as Telnet, unencrypted HTTP, or FTP shall be disabled unless explicitly required, risk-justified, and protected by compensating controls. Equivalent controls for provider-managed environments shall be addressed through due diligence, contractual assurance, or technical evidence.

9.4 DEFAULT ACCOUNTS AND SETTINGS

Default accounts shall be disabled, renamed, or otherwise secured. Default passwords shall be changed before deployment. Any retained default or embedded account shall be documented together with the business justification, access restriction, monitoring, and compensating controls.

9.5 BROWSERS, EMAIL, DNS FILTERING, AND ANTI-MALWARE

Only supported and up-to-date browsers and email clients shall be used on enterprise systems. Automatic or centrally managed updates shall be enabled where feasible. DNS filtering shall be used to block known malicious or unauthorized domains and shall be monitored to avoid interference with legitimate gaming and regulatory services.

Supported endpoints and servers administered by the Company shall be protected by centrally managed anti-malware or endpoint detection controls with automatic updates and regular scanning. For provider-managed systems, the Company shall obtain appropriate assurance that

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

equivalent controls are maintained. Security tools shall be configured and tested to avoid unacceptable impact on gaming systems and critical operations.

9.6 REMOVABLE MEDIA

Automatic execution from removable media shall be disabled. Use of removable storage shall be limited to authorized business purposes, subject to approval and technical controls. Removable media shall be scanned or validated before use, and sensitive data shall be encrypted where storage on approved removable media is unavoidable.

10. ACCOUNT, ACCESS, AND AUTHENTICATION MANAGEMENT

10.1 ACCOUNT INVENTORY AND LIFECYCLE

The Company shall ensure that a complete inventory is maintained for user, service, system, and administrative accounts within the applicable responsibility scope. The inventory shall include the account owner, username or identifier, role or department, privilege level, creation date, and deactivation date where applicable. Active accounts shall be reviewed at least quarterly to confirm validity and necessity. Provider-managed account records may be maintained by the provider, provided that the Company has appropriate access to assurance or evidence.

Access shall be provisioned through a documented and auditable process requiring appropriate approval. Changes in employment, duties, contractual status, or business need shall trigger access review. Access shall be revoked or adjusted promptly upon termination, contract completion, or role change, and accounts should be disabled rather than deleted where audit history must be retained.

10.2 PASSWORDS AND AUTHENTICATION

Passwords for accounts administered by the Company shall be strong, unique, and confidential. Shared and default passwords are prohibited except for approved service accounts subject to compensating controls and controlled credential management. Accounts protected by MFA shall use passwords of at least eight (8) characters; accounts not protected by MFA shall use passwords of at least fourteen (14) characters. Password managers should be used or made available to support unique credential storage. For provider-managed authentication, the Company shall require or verify equivalent or stronger authentication standards.

10.3 DORMANT ACCOUNTS

Inactive accounts administered by the Company shall be monitored and disabled after forty-five (45) days of non-use unless a documented business exception applies. Reactivation shall require validation and appropriate approval. Seasonal or exceptional accounts shall have documented expiry or review dates. Provider-managed environments shall be subject to equivalent lifecycle controls or documented assurance.

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.**10.4 PRIVILEGED ACCOUNTS AND SEPARATION OF DUTIES**

Privileged access shall be assigned only to dedicated administrative accounts and used only for authorized elevated functions. Administrative accounts shall not be used for routine email, web browsing, or ordinary document activities. Administrative and standard user activities shall be separated, and access to gaming systems, player data, financial systems, and security tools shall be subject to enhanced logging and review.

10.5 MULTI-FACTOR AUTHENTICATION

Multi-factor authentication ("MFA") shall be required for all internet-facing or externally accessible business applications and portals, remote access methods including VPN or remote desktop, and administrative access to core gaming systems and infrastructure. Approved methods may include authenticator applications, hardware security tokens, or suitable biometric controls. Where authentication is managed by a provider, the Company shall require or verify equivalent MFA coverage through contractual assurance, due diligence, or technical evidence. Exceptions shall be documented, time-limited, risk-approved, and supported by compensating controls.

11. VULNERABILITY AND PATCH MANAGEMENT**11.1 VULNERABILITY MANAGEMENT**

The Company shall maintain a risk-based vulnerability management process covering operating systems, networks, web applications, cloud resources, third-party software, and systems within its responsibility. Vulnerability scanning shall be conducted at least monthly and more frequently for critical or internet-facing systems where warranted by risk. For provider-managed environments, the Company shall obtain appropriate assurance regarding vulnerability identification, prioritization, and remediation.

Vulnerabilities shall be evaluated and prioritized based on severity, exploitability, asset criticality, exposure, threat intelligence, player impact, gaming integrity, and regulatory consequences. Remediation shall be time-bound and tracked. Exceptions shall require documented risk acceptance, compensating controls, and a review date.

11.2 PATCH MANAGEMENT

Operating system, software, application, firmware, and network patches for systems within the Company's responsibility shall be reviewed and applied at least monthly or sooner where critical risk, active exploitation, or vendor guidance requires accelerated action. Updates shall be tested in a staging or non-production environment where practicable before production deployment. Approvals, deployment outcomes, failures, and exceptions shall be documented. For provider-managed systems, the Company shall monitor patching obligations and obtain appropriate evidence or assurance.

Patch schedules shall be coordinated to minimize disruption to gaming services, financial processing, and regulatory reporting. Dependencies involving certified systems or third-party

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

platforms shall be managed with the relevant provider, without reducing the Company's obligation to exercise due diligence, verify material remediation, and monitor risks within the shared responsibility model.

12. LOGGING, MONITORING, AND AUDIT TRAILS

12.1 LOG MANAGEMENT

The Company shall define and maintain, directly or through relevant service providers, logging requirements for critical systems, business applications, security tools, databases, endpoints, cloud services, and administrative activities. Requirements shall address log generation, collection, retention, review, access, integrity, archival, and secure disposal within the applicable responsibility scope.

Audit logs shall be enabled on enterprise assets within the applicable responsibility scope and, where feasible, forwarded to centralized or otherwise protected storage. Logs shall be protected against unauthorized alteration or deletion through access controls, cryptographic integrity methods, write-once controls, or equivalent safeguards. Access to logs shall be restricted to authorized personnel. For provider-managed systems, the Company shall require appropriate logging and access to relevant records or assurance.

12.2 GAMING AND REGULATORY EVENTS

Logging shall include, where applicable:

- Player authentication, account changes, and security-relevant account activity;
- Deposits, withdrawals, transfers, wagers, payouts, reversals, and high-value events;
- Gameplay, tournament, hand-history, and gaming integrity events where relevant;
- Administrative access, privilege use, configuration changes, and security control changes;
- KYC/CDD, AML, sanctions, Responsible Gaming, complaints, and investigation events;
- Security alerts, malware detections, access failures, network anomalies, and incident response actions; and
- Regulatory submissions, reporting references, and evidence relevant to CGA or FIU oversight.

Logs shall be reviewed periodically and when alerts, incidents, unusual activity, regulatory requests, or material changes arise. Retention shall reflect legal, regulatory, security, audit, and operational requirements, including the minimum retention applicable to regulated records.

13. NETWORK AND INFRASTRUCTURE SECURITY

The Company shall ensure that an inventory is maintained for network infrastructure within its responsibility, including routers, switches, firewalls, gateways, remote access services, and security appliances. Firmware and software support status shall be reviewed at least monthly, and updates shall be applied according to vendor guidance and risk. Provider-managed infrastructure shall be addressed through documented responsibility allocation, due diligence, and appropriate assurance.

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

Network access within the Company's responsibility shall be restricted to authorized services and users. Appropriate segmentation, firewalling, secure remote access, encrypted management, and monitoring controls shall be used to reduce unauthorized access and limit the impact of compromise. Remote administrative access shall require MFA and shall be logged. Equivalent outcomes for provider-managed networks shall be required or verified through contractual and technical assurance.

Network changes shall be authorized and documented. Unsupported or end-of-life infrastructure shall not remain in production unless subject to a documented, approved exception with compensating controls and a remediation plan.

14. CRYPTOGRAPHIC CONTROLS AND DATA MASKING

The Company shall ensure, directly or through relevant service providers, that sensitive player, financial, gaming, security, and regulatory information is encrypted in transit and at rest using secure, industry-standard cryptographic protocols and algorithms appropriate to the risk and technology. Company-administered laptops, tablets, and mobile devices that store or process sensitive or regulated data shall use full-disk encryption.

Encryption keys, certificates, secrets, and tokens shall be generated, stored, used, rotated, revoked, archived, and retired securely. Access shall be restricted and auditable. The Company shall maintain sufficient records of material cryptographic controls and approved exceptions.

Personal data, credentials, transaction information, gaming data, and other sensitive information used in development, testing, quality assurance, analytics, or training environments shall be masked, tokenized, anonymized, or replaced with non-production data unless use of production information is specifically authorized and protected.

15. BACKUP, RECOVERY, BUSINESS CONTINUITY, AND OPERATIONAL RESILIENCE

15.1 BACKUP AND RECOVERY

The Company shall identify, directly or through relevant service providers, the systems and data requiring backup, with priority given to critical gaming operations, player accounts, transaction records, configuration data, regulatory records, logs, and information necessary to restore lawful operations.

Backups shall be automated where feasible and performed at least weekly within the applicable responsibility scope. Critical gaming transaction logs, financial data, player balances, and other high-volume or high-impact information shall be backed up more frequently, including daily or near-real-time where required to prevent unacceptable data loss or meet regulatory obligations. For provider-managed systems, the Company shall verify backup obligations through contractual assurance, service documentation, testing evidence, or other appropriate records.

Backup information shall be encrypted where appropriate, access-restricted, monitored, and protected from alteration or ransomware through offline, off-site, immutable, logically isolated,

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

or equivalent safeguards. Backup protection shall be equivalent to the protection applied to the original data.

Recovery arrangements shall define system priority, responsibilities, dependencies, recovery point objectives ("RPOs"), recovery time objectives ("RTOs"), and restoration validation, taking account of provider service levels and dependencies where relevant. Restoration testing shall be performed at least annually and after material changes. Test results and corrective actions shall be documented or otherwise evidenced through relevant provider records.

15.2 BUSINESS CONTINUITY AND OPERATIONAL ASSURANCE

Information security shall be integrated into business continuity and disaster recovery arrangements. Critical processes shall have documented fallback, redundancy, failover, or manual procedures appropriate to their risk, including player account access, transaction processing, security monitoring, regulatory reporting, and communications. Such arrangements may be maintained directly by the Company, by relevant service providers, or through coordinated shared-responsibility procedures.

Continuity and recovery arrangements shall be reviewed and tested at least annually or following material operational, provider, system, or regulatory changes. Changes to critical systems shall be subject to security and continuity risk assessment. Sensitive data used during tests or audits shall be masked and access-controlled. The Company may rely on provider testing evidence where the provider operates the relevant system, subject to due diligence and assessment of adequacy.

16. THIRD-PARTY, CLOUD, AND B2B PROVIDER SECURITY

16.1 REGULATORY ACCOUNTABILITY AND SHARED RESPONSIBILITY

The Company may rely on B2B platforms, cloud providers, hosting services, game suppliers, payment processors, KYC vendors, security providers, data providers, and other service providers. Contractual or operational delegation shall not transfer the Company's regulatory accountability under the LOK. The Company shall remain responsible for due diligence, verification, contractual assurance, monitoring, incident escalation, and regulatory notification within the shared responsibility model, while providers remain responsible for the controls and systems allocated to them.

16.2 PROVIDER INVENTORY AND DUE DILIGENCE

The Company shall maintain a current inventory of material service providers, including the services provided, internal owner, systems or data accessed, data exchanged, hosting or processing location where relevant, security and incident obligations, audit or certification status, and contractual termination or exit considerations. The inventory may be supported by contracts, due diligence records, architecture documentation, or other provider records and shall be reviewed at least annually and when providers or services change.

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

Security due diligence shall be completed before onboarding material providers and periodically thereafter based on risk. Due diligence may include review of security controls, certifications, independent reports, incident history, business continuity, data protection, access controls, subcontractors, and regulatory status. The nature and depth of evidence obtained shall reflect the criticality of the service and the Company's ability to exercise direct control.

16.3 CONTRACTUAL SECURITY REQUIREMENTS

Material Service Provider agreements shall include appropriate confidentiality, information security, access control, data protection, incident notification, business continuity, audit or evidence rights, regulatory cooperation, data return or deletion, subcontractor, and termination requirements. Where legacy or standard-form agreements do not contain every preferred term, the Company shall assess the risk, document available assurances and compensating measures, and pursue remediation where material. Providers shall notify the Company promptly of incidents, certification lapses, material control failures, or changes affecting regulated services.

16.4 CERTIFIED B2B PROVIDERS AND GAME CONTENT

Where the Company uses certified Remote Gaming Servers, game content, or components supplied by a licensed B2B provider, the provider retains responsibility for obtaining and maintaining its required certifications. The Company shall verify certification status at onboarding and at least annually, maintain contractual requirements for continued certification and notification of changes, notify the CGA when it becomes aware of a relevant lapse or withdrawal, and cease use of affected components until valid certification is restored where required.

16.5 EXTERNALLY SUPPLIED DATA AND FEEDS

Where third-party data feeds or aggregated content influence wager or game outcomes, connections shall use authenticated and encrypted channels. Integrity safeguards such as digital signatures, hashes, message authentication codes, or equivalent controls shall be used where applicable. Availability, latency, consistency, and anomalies shall be monitored. The Company shall be able to suspend affected offerings when data integrity cannot be assured and resume only after integrity is re-established.

17. SECURITY INCIDENT MANAGEMENT AND CGA NOTIFICATION

17.1 INCIDENT RESPONSE ROLES AND CONTACTS

The Company shall designate a primary and backup incident response coordinator and define responsibilities for technical response, containment, recovery, legal analysis, compliance, regulatory communication, player communication, and management oversight. An up-to-date incident contact directory shall include internal stakeholders, critical providers, the CGA,

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

relevant authorities, legal counsel, insurers where applicable, and forensic support resources. Contact information may be maintained in a separate controlled operational record.

17.2 REPORTING AND RESPONSE PROCESS

All personnel and service providers shall report actual or suspected security incidents without delay through approved channels. The Company shall document, maintain, and apply an incident response process appropriate to its operating model and provider dependencies that includes:

1. Identification and Triage: confirm the event, affected systems, data, players, transactions, providers, and regulatory implications;
2. Containment: limit unauthorized access, manipulation, data loss, fraud, or service disruption;
3. Preservation of Evidence: secure logs, records, system images, communications, and other relevant evidence;
4. Investigation and Assessment: determine cause, scope, impact, affected information, and whether gaming integrity, player funds, personal data, reporting, availability, or fairness is affected;
5. Eradication and Recovery: remove the cause, remediate vulnerabilities, restore services safely, and monitor for recurrence;
6. Notification and Communication: notify management, affected providers, the CGA, authorities, and affected persons where required; and
7. Post-Incident Review: document lessons learned, corrective actions, responsible owners, and completion dates.

17.3 MANDATORY CGA NOTIFICATION

The Company shall notify the Curaçao Gaming Authority without undue delay and, in any event, within twenty-four (24) hours of becoming aware of a security incident that:

- Compromises or may compromise gaming integrity;
- Affects or may affect player funds or personal data;
- May impact regulatory reporting, system availability, or game fairness; or
- Otherwise meets a CGA reporting requirement or presents a material regulatory risk.

The initial notification may be supplemented as the investigation develops. Records of the incident, assessment, decisions, notifications, evidence, recovery, and corrective actions shall be retained and made available to the CGA upon request.

18. PHYSICAL AND HUMAN RESOURCE SECURITY

18.1 PHYSICAL AND ENVIRONMENTAL SECURITY

Physical access to offices, equipment, server or network areas, records, and other sensitive locations shall be limited to authorized persons. Appropriate access controls, visitor

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

management, entry records, surveillance where applicable, clean desk and clear screen practices, secure equipment storage, and environmental safeguards shall be implemented based on risk. Company equipment used off-premises shall be protected against loss, theft, unauthorized access, and damage. Sensitive information shall not be left unattended or displayed where unauthorized persons may view it.

18.2 HUMAN RESOURCE SECURITY

Security responsibilities shall be managed throughout the employment and contracting lifecycle. Background checks shall be conducted for new personnel in critical or sensitive roles where lawful and appropriate. Employment and contractor arrangements shall include confidentiality and security obligations.

Personnel shall acknowledge security responsibilities during onboarding. Failure to comply may result in disciplinary or contractual action. On termination or role change, Company assets shall be returned, access shall be revoked or adjusted promptly, and continuing confidentiality obligations shall be reinforced.

19. SECURITY AWARENESS AND ROLE-BASED TRAINING

All personnel shall receive baseline information security awareness training during onboarding and at least annually thereafter. Additional training shall be provided when material policies, threats, technologies, systems, or regulatory requirements change.

Training shall address, as applicable:

- Secure use of Company systems, devices, software, and information;
- Phishing, business email compromise, social engineering, and fraud;
- Password security, MFA, credential protection, and privileged access;
- Secure storage, transmission, sharing, retention, and disposal of data;
- Prevention of accidental disclosure, misdelivery, and data loss;
- Identification and immediate reporting of security incidents;
- Remote work, insecure networks, removable media, and physical security;
- Gaming-specific threats, player data protection, game integrity, transaction manipulation, account compromise, and regulatory obligations.

Personnel with elevated security responsibilities shall receive additional role-based training. Training completion shall be documented and retained.

20. COMPLIANCE MONITORING, AUDIT, REVIEW, AND EXCEPTIONS

20.1 COMPLIANCE EVIDENCE AND SELF-ASSESSMENT

The Company shall maintain or obtain evidence demonstrating implementation and operation of applicable controls, including inventories, reviews, approvals, access records, scan and patch results, incident records, training records, backup tests, provider reviews, certifications, service

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

reports, and corrective actions. Evidence may be generated internally or maintained by relevant service providers and shall be retained according to applicable legal and regulatory requirements. The Company shall complete annual information security self-assessments using CGA templates or other required formats and shall cooperate with CGA reviews, inspections, technical validation, document requests, configuration testing, remote assessments, and spot checks.

20.2 INDEPENDENT SECURITY AUDIT

As an online operator, the Company shall undergo independent third-party security audits when and to the extent required by the CGA or applicable license conditions. Audit scope shall reflect the Company's operating model, systems, providers, player data, gaming services, and regulatory obligations. Findings shall be documented, assigned, prioritized, remediated, and monitored through completion.

20.3 POLICY REVIEW AND CONTINUOUS IMPROVEMENT

This Policy and the effectiveness of its controls shall be reviewed at least annually and when significant changes occur to laws, CGA requirements, systems, providers, threats, incidents, products, services, operations, or organizational responsibilities. Reviews shall be approved by senior management and documented.

The Company shall monitor corrective actions and improve its security posture over time. CIS IG1 shall remain the mandatory baseline, while progression toward appropriate IG2 maturity shall be considered as a strategic objective based on risk, resources, and CGA guidance.

20.4 POLICY EXCEPTIONS

Exceptions to this Policy shall be limited, documented, time-bound, risk-assessed, and approved by the appropriate technical owner and management, with Compliance involvement where regulatory requirements may be affected. The exception shall identify the affected requirement, business rationale, risk, compensating controls, owner, approval date, expiry or review date, and remediation plan. Mandatory CGA obligations shall not be waived through internal exception approval.

21. ENFORCEMENT AND NON-COMPLIANCE

Failure to comply with this Policy may expose the Company, its players, and its licensed operations to financial, legal, regulatory, operational, and reputational harm. Non-compliance may result in corrective action, access restriction, disciplinary measures, contract remedies, termination, regulatory reporting, or other action appropriate to the nature and severity of the matter.

Suspected intentional violations, concealment of incidents, unauthorized access, interference with logs or evidence, circumvention of security controls, misuse of privileged access, or unauthorized disclosure of sensitive or regulated information shall be escalated immediately to management, Compliance, and the designated information security function.

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

The Company shall cooperate fully with CGA investigations, remediation requirements, compliance orders, audits, and deadlines. Failure to comply with CGA information security requirements may result in regulatory enforcement, including warnings, financial penalties, enhanced security obligations, suspension, or revocation of the license.

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

APPENDIX A - MINIMUM CONTROL FREQUENCIES

The following minimum frequencies apply unless a stricter legal, regulatory, risk-based, contractual, or technical requirement applies:

Control Or Activity	Minimum Frequency / Deadline
Enterprise device inventory review	At least twice annually
Unauthorized device identification and response	Weekly
Software inventory review	At least twice annually
Software and network support status review	Monthly
User and privileged account review	Quarterly
Dormant account disablement	After 45 days of non-use, unless approved exception
Vulnerability scanning	At least monthly; more frequently for critical systems
Patch review and deployment	At least monthly; accelerated for critical risk
Backup execution	At least weekly; daily or near-real-time for critical data as required
Backup restoration testing	At least annually and after material changes
Security awareness training	At onboarding and at least annually
Service provider inventory review	At least annually and upon material change
B2B certification verification	At onboarding and at least annually
Information security risk assessment	At least annually and upon material change
Policy and control review	At least annually and upon material change
CGA notification for reportable security incidents	Without undue delay and within 24 hours

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

APPENDIX B - DATA CLASSIFICATION AND HANDLING SUMMARY

Data Category	Classification	Minimum Handling Standard
Critical Gaming and Regulatory Data	Restricted	Strict need-to-know; encryption; logging; regulatory retention; controlled sharing.
Player Personal and Financial Data	Restricted	Role-based access; encryption in transit and at rest; approved systems only; regulated retention and secure disposal.
Business Confidential Information	Confidential	Authorized personnel and providers only; approved storage and transfer; contractual confidentiality.
Internal Information	Internal	Company and authorized provider use; no unauthorized public disclosure.
Public Information	Public	Approved for public disclosure; integrity and publishing controls apply.

INFORMATION SECURITY POLICY - KING ENTERPRISES N.V.

APPENDIX C - REPORTABLE SECURITY INCIDENT CRITERIA

An incident shall be escalated immediately for regulatory assessment and may require notification to the CGA within twenty-four (24) hours where it involves or may involve:

- Unauthorized access to player, financial, gaming, security, AML, KYC/CDD, Responsible Gaming, complaints, or regulatory data;
- Loss, theft, disclosure, corruption, encryption, or destruction of sensitive or regulated data;
- Compromise, manipulation, or suspected manipulation of game outcomes, transactions, player balances, payouts, RNG-related records, or gaming data feeds;
- Fraud, account compromise, privileged access misuse, or unauthorized configuration change affecting regulated systems;
- Material malware, ransomware, denial-of-service, network compromise, or service outage;
- Failure or compromise affecting regulatory reporting, audit logs, FIU-related processes, or CGA access to records;
- A material third-party or cloud provider incident affecting Company operations, data, or compliance; or
- Any event that may materially affect game fairness, player funds, personal data, system availability, or the Company's ability to comply with the LOK or CGA requirements.

APPROVAL AND SIGNATURE

This Policy is approved and signed by Charles N. Porter, on behalf of Local Partners B.V., as Managing Director. The Policy is the governing approval instrument for the Information Security Governance Framework and its controlled supporting documents. Effective Date: May 10, 2026. Version 1.1 last updated July 21, 2026. The signed version shall be maintained as part of the Company's official governance and regulatory records and made available to the Curaçao Gaming Authority upon request.

Signed by:

Charles N. Porter

A854D04785BD4EC...

CHARLES N. PORTER

On behalf of Local Partners B.V.
Managing Director