

NEW ORIGIN B.V.

Information Security Policy

Prepared for Curaçao licensing submission

Operator	New Origin B.V.
Brand / Domain	ohmywin.com (and associated domains)
Jurisdiction	Curaçao
Version	1.2
Classification	Internal / Licensing Submission

This document forms the standalone Information Security Policy for New Origin B.V. and is intended for internal governance and licensing submission purposes.

Document Control

Operator	New Origin B.V.
Brand / Domain	ohmywin.com (and associated domains)
Jurisdiction	Curaçao
Version	1.2
Effective Date	20 April 2026
Document Owner	Raúl Moreno López (acting as Privacy & Security Owner)
Approved By	Allyant Group B.V., represented by Philip M. Humme (Managing Director)
Classification	Internal / Licensing Submission
Reference	New Origin B.V. – Information Security Policy v1.2

Version History

Version	Summary of Change	Date	Status
1.0	Initial draft prepared for Curaçao licensing submission	17 April 2026	Superseded
1.1	Updated provider stack and refined governance language for current operating model	20 April 2026	Superseded
1.2	Closed approval data, aligned provider stack with current business plan, and confirmed control baselines and review cadence	20 April 2026	Current

Approval / Sign-off

Role	Name	Date / Signature
Document Owner	Raúl Moreno López (acting as Privacy & Security Owner)	20 April 2026
Approver	Philip M. Humme on behalf of Allyant Group B.V. (Managing Director)	20 April 2026

Contents Overview

- | | |
|---|---|
| 1. Purpose | 12. Software Development, Change Management and Release Control |
| 2. Scope | 13. Incident Detection, Reporting and Response |
| 3. Definitions | 14. Business Continuity, Backups and Disaster Recovery |
| 4. Responsibility and Governance | 15. Third-Party and Outsourcing Security |
| 5. Information Security Risk Management | 16. Employee / Contractor Awareness, Confidentiality and Training |
| 6. Risk Themes Considered | 17. Monitoring, Logging and Record Retention |
| 7. Access Control and Identity Management | 18. Policy Breaches and Escalation |
| 8. Data Classification, Data Protection and Privacy | 19. Review, Approval and Version Control |
| 9. System, Infrastructure and Network Security | Appendix A – Open Points to Confirm Before Approval |
| 10. Endpoint Security and Secure Remote Access | Appendix B – Supporting Records Expected to Exist |
| 11. Encryption and Secure Data Handling | |

1. Purpose

The purpose of this Information Security Policy is to define the minimum governance, organisational, procedural and technical controls by which New Origin B.V. protects its information assets, systems, services, records and operational resilience.

This Policy is intended to support the Company's regulated online gaming activities and to ensure that information security is managed in a manner proportionate and appropriate for a Curaçao-licensed operator operating a vendor-supported model. It is designed to protect, at a minimum, player data, KYC and AML/CFT records, payment-related information, business-sensitive information, security logs, operational records and the availability and integrity of critical services.

This Policy is intended to remain consistent with the Company's KYC Policy, Terms & Conditions, AML/CFT/CFP Manual, Responsible Gaming Policy, Complaints Policy and other related internal controls.

2. Scope

This Policy applies to New Origin B.V., its brands, domains, operational environments, supporting systems, administrative tools, records, and all information processed in connection with its regulated activities.

It applies to all directors, officers, employees, contractors, temporary personnel, and relevant third-party service providers that host, process, transmit, administer, support, monitor, or may otherwise have access to Company systems, Company data, or security-relevant operational environments.

For the Company's current operating model, this includes, in particular, the core platform, gaming content aggregation, payment and cashier-related arrangements, customer support systems, communications tools, compliance support tools, monitoring and logging environments, and any other ancillary systems or providers used in the delivery, administration, support, control, or oversight of the business.

Without limiting the generality of the above, the Company's current critical outsourced service stack includes:

- GiG Software CoreX as core platform provider;
- GiG Software SportX as sportsbook provider;
- Alea as game aggregation provider;
- Merchant Connect as payment aggregation / gateway provider;
- AgeChecked as age-verification provider;
- Sendgrid as email / EMS provider; and
- Zendesk as customer support / live chat provider.

This Policy is intended to apply both to current arrangements and to any future approved replacement, successor, supplementary, or additional provider performing materially equivalent functions for the Company.

3. Definitions

For the purposes of this Policy:

Information Asset means any data, record, system, application, configuration, credential, log, report, document or technology resource owned, controlled or used by the Company.

Security Incident means any event that actually or potentially compromises the confidentiality, integrity or availability of information, systems or services, including cyberattack, malware event, ransomware event, account compromise, unauthorised access, data leakage, service outage, fraudulent misuse, credential exposure or material third-party failure.

Privileged Access means administrative, root, superuser, elevated or otherwise enhanced access capable of materially changing systems, configurations, security settings, user rights or operational data.

Personal Data means information relating to an identified or identifiable individual, including player, staff, contractor or counterparty information.

Restricted Data means information requiring the highest level of protection, including KYC documentation, AML/CFT case records, suspicious activity escalations, payment ownership evidence, security credentials, incident records and privileged system information.

4. Responsibility and Governance

New Origin B.V. operates a lean governance model supported by specialist outsourced providers. Information security shall therefore be governed through clear accountability, documented oversight, functional segregation, and proportionate escalation routes.

Overall accountability for information security rests with the Managing Director and Board-level management, who shall ensure that the Company maintains appropriate information security governance, oversight, resourcing, and internal controls proportionate to its business model, operational scale, outsourcing structure, and regulatory obligations.

The Privacy & Security Owner is responsible for day-to-day oversight of information security matters, including access governance, data handling oversight, retention practices, incident coordination, follow-up on security issues, and internal coordination with relevant business and control functions.

The COO, acting as Platform Owner, is responsible for operational governance of critical technology and service providers, including platform, gaming aggregation, payments, and related service providers, and for coordinating release oversight, service escalation, issue tracking, and resolution follow-up where operational, technical, or security concerns affect the business.

The Compliance Officer shall be consulted where a security matter has regulatory, KYC, AML/CFT, customer verification, retention, outsourcing, or policy-governance implications.

The MLRO shall be involved without delay where a security incident or security concern may also involve suspicious activity, fraud, sanctions, source-of-funds concerns, compromise of AML/CFT records, unlawful access to compliance information, or any matter requiring legal or regulatory escalation.

The Payments & Risk Owner shall be involved in payment-security matters, transaction anomalies, payment-method ownership concerns, chargeback abuse patterns, or other events affecting the security, integrity, or control of payment-related operations.

Third-party providers may implement, operate, or support technical, hosting, payment, content-delivery, monitoring, administrative, or security-relevant functions; however, New Origin B.V. remains ultimately responsible for information security governance, oversight, and final decision-making.

5. Information Security Risk Management

The Company shall maintain a risk-based information security approach.

At a minimum, the Company shall:

- identify relevant security threats, vulnerabilities, dependencies and control weaknesses;
- assess the likelihood and potential impact of those risks;
- record material risks in a risk register or equivalent control record;
- assign an owner for remediation or mitigation;
- track status and follow-up actions; and
- review the assessment at least annually and additionally when triggered by material change.

Risk reviews shall also be performed following material changes to the operating model, onboarding or termination of critical vendors, major system or product changes, incidents or near misses, entry into new markets or payment channels, or material regulatory or contractual developments.

6. Risk Themes Considered

The Company's information security risk management framework shall consider, at a minimum, threats and vulnerabilities relating to:

- cyberattack, attempted intrusion, and service disruption;
- phishing, social engineering, and business email compromise;
- ransomware, malware, and endpoint compromise;
- credential exposure, account compromise, and misuse of privileged access;
- insider misuse, human error, and unauthorised activity;
- data leakage, confidentiality breaches, and unauthorised disclosure;
- payment abuse, transaction manipulation, or compromise of cashier-related processes;
- third-party failure, vendor compromise, or dependency risk affecting critical services;
- weaknesses in system configuration, access control, release management, monitoring, backup, or recovery processes;

- elevated risk factors associated with high-value, high-frequency, or higher-touch customer segments, including VIP relationships from launch; and
- any other threat, vulnerability, dependency, or control weakness that may materially affect the confidentiality, integrity, availability, auditability, or resilience of the Company's regulated operations.

The Company's risk reviews shall remain proportionate and may be adapted over time to reflect operational evolution, changes in providers, new products, changing payment methods, incident history, emerging threats, or changes in legal or regulatory expectations.

7. Access Control and Identity Management

Access to systems, data, back-office environments, and security-relevant tooling shall be granted on the basis of business need, role, least privilege, and appropriate approval.

The Company shall maintain the following principles:

- access shall be role-based wherever reasonably practicable;
- elevated or privileged access shall be limited to authorised personnel with a legitimate operational, technical, security, or compliance need;
- user access shall be approved, modified, reviewed, and removed through controlled processes proportionate to the relevant system and risk;
- access to KYC, AML/CFT, payment, complaints, responsible gaming, and other sensitive records shall be limited on a need-to-know basis;
- privileged actions, material configuration changes, and administrative access events shall be logged where supported by the relevant environment; and
- stronger authentication measures, including multi-factor authentication where available and appropriate, shall be used for privileged access, sensitive administrative access, remote access, or other higher-risk access scenarios.
- joiner, mover and leaver access changes shall be actioned without undue delay;
- privileged access shall be reviewed at least quarterly; and
- other sensitive administrative access shall be reviewed at least annually, or more frequently where justified by risk or system criticality.

Where a system or provider does not natively support a desired access-control feature, the Company may apply compensating controls appropriate to the relevant risk, provider model, and operational reality.

8. Data Classification, Data Protection and Privacy

The Company shall classify and protect information according to its sensitivity, business criticality, regulatory relevance, and operational risk. At minimum, information may be treated as Public, Internal, Confidential or Restricted.

The following shall ordinarily be treated as Restricted or subject to enhanced protection:

- player identification and KYC documents;
- AML/CFT case files, suspicious activity escalations, sanctions-related records, and source-of-funds or source-of-wealth information;
- payment-related records and payment ownership evidence;
- security credentials, privileged access information, and incident records;
- complaints, responsible gaming interventions, and other regulated case records where sensitive or investigative in nature; and
- logs, internal reports, or operational records that could materially affect security, investigations, or compliance if disclosed inappropriately.

The Company shall process, retain, archive, restrict, disclose, or securely delete information in accordance with its legal, regulatory, contractual, and operational requirements. Retention periods and record retrievability shall remain aligned with the wider Company framework, which generally requires material operational, customer, compliance, complaints, communications, and AML/CFT-related records to remain available for at least five years, subject to longer retention where required by law, investigation, reporting, audit, or authority request.

9. System, Infrastructure and Network Security

The Company shall maintain a proportionate set of technical and organisational safeguards designed to protect its systems, services, administrative environments, and regulated operations.

Given the Company's outsourced operating model, many technical controls may be implemented directly by the Company, by critical service providers, or within vendor-managed environments. The Company shall nevertheless maintain oversight, governance, and escalation arrangements designed to ensure that the overall control environment remains appropriate to the business.

The Company's security framework shall include, as applicable and proportionate:

- secure configuration standards for Company-managed systems and devices;
- firewall, filtering, or equivalent perimeter protections where relevant;
- endpoint protection and anti-malware measures for Company-managed devices where applicable;
- patching, version management, or other maintenance processes for Company-managed systems;
- vulnerability identification and remediation, whether directly or through providers;
- restricted administrative interfaces and controlled access to back-office environments;
- secure remote access arrangements;
- monitoring of critical systems, administrative activity, security events, and material service interruptions; and
- logging of privileged actions, configuration changes, and other relevant administrative events where supported.

For the Company's current operating model, the following providers shall be treated as critical vendors from an information security perspective:

- GiG Software CoreX as core platform provider;
- GiG Software SportX as sportsbook provider;
- Alea as game aggregation provider;
- Merchant Connect as payment aggregation / gateway provider;
- AgeChecked as age-verification provider;
- Sendgrid as email / EMS provider; and
- Zendesk as customer support / live chat provider.

The Company shall seek reasonable assurance, appropriate to the circumstances, that critical providers maintain suitable controls relating to security, resilience, access restriction, incident handling, service continuity, auditability, and record retrievability in relation to the services they provide.

10. Endpoint Security and Secure Remote Access

All personnel accessing Company administrative systems, back-office tools or sensitive data shall do so only through approved channels.

The Company shall apply the following minimum expectations:

- only authorised personnel may access administrative systems;
- devices used for administrative or privileged access shall be protected by password or equivalent authentication, updated software and reasonable endpoint hygiene;
- remote access to critical systems shall use encrypted connections and, where supported, stronger authentication controls and restricted access paths;
- access from clearly unsafe or uncontrolled environments shall not be permitted for privileged activity; and
- downloads or local storage of Restricted data shall be minimised and controlled.

11. Encryption and Secure Data Handling

The Company shall protect sensitive data in transit and at rest through proportionate security measures appropriate to the nature of the information, the relevant systems, the delivery model, and the level of risk.

At minimum:

- sensitive information transmitted across public or untrusted networks shall be protected using secure transport methods where appropriate;
- sensitive stored information, backups, and vendor-held records shall be protected by encryption, logical segregation, or equivalent safeguards where appropriate and supported;

- credentials, secrets, keys, tokens, and other security-sensitive information shall not be stored, shared, or transmitted insecurely;
- Restricted data shall not be exported, distributed, or transmitted through unauthorised channels except where justified, controlled, and appropriately protected; and
- use of live or production data in non-production environments shall be minimised and controlled.

The Company may apply equivalent or compensating safeguards where a particular environment, vendor solution, or technical architecture does not use identical control methods but achieves materially similar protection.

12. Software Development, Change Management and Release Control

The Company relies materially on third-party platforms, managed services and vendor-supported environments. Information security shall therefore be embedded into change and release governance.

All material system changes, configuration changes, integrations and production releases shall be subject to a documented process that includes, as appropriate:

- request or identification of the change;
- review of operational, security and compliance impact;
- approval by the relevant system owner or delegated approver;
- testing prior to production deployment;
- controlled deployment;
- rollback or recovery planning where feasible; and
- post-change review where justified by risk or incident history.

Emergency changes may be implemented where necessary to protect security, stability or compliance, but shall be documented and reviewed after implementation.

13. Incident Detection, Reporting and Response

All personnel and relevant service providers shall report actual or suspected security incidents without undue delay.

A security incident may include, without limitation:

- unauthorised or suspicious access;
- compromise of credentials or accounts;
- data loss, leakage, corruption, or unauthorised disclosure;
- malware, ransomware, or endpoint compromise;
- service outage or material availability issue;
- unauthorised change to configuration or controls;
- third-party breach or incident affecting Company systems, data, payments, or regulated operations; and
- payment-security events, transaction-integrity concerns, or other security-related fraud indicators.

The Company shall maintain an incident response process covering, as appropriate: detection and internal reporting, initial triage and classification, containment and protective action, investigation and evidence preservation, remediation and recovery, internal escalation to relevant management and control functions, external notification where legally or contractually required, and post-incident review with lessons learned.

An incident register or equivalent record shall be maintained, capturing the incident, affected areas, actions taken, escalation, outcome, and lessons learned.

14. Business Continuity, Backups and Disaster Recovery

The Company shall maintain business continuity and recovery arrangements proportionate to its operational reliance on outsourced platform, gaming aggregation, payment, and support providers.

At a minimum:

- critical systems and regulated records shall be backed up daily or according to system criticality and relevant provider arrangements;
- backup responsibilities may be allocated between the Company and relevant providers depending on the relevant environment and service model;
- for the current operating model, daily backups or provider-equivalent backup arrangements are expected for critical regulated records and administrative data, subject to documented system criticality and vendor design;

- backups shall be stored securely and protected against unauthorised access, alteration, or deletion;
- restoration capability shall be tested at least semi-annually for Company-controlled critical data and systems, and otherwise through annual assurance, testing evidence, or service oversight obtained from relevant critical providers;
- critical outages or incidents affecting player services, platform availability, gaming delivery, payment routing, KYC or AML documentation, complaints data, or material logs shall be escalated without undue delay and tracked through to resolution; and
- recovery priorities shall take into account regulatory, operational, customer, financial, and investigatory requirements.

15. Third-Party and Outsourcing Security

Because the Company operates a specialist outsourced model, third-party security governance is a core control.

Before onboarding any critical or sensitive provider, the Company shall perform proportionate due diligence taking into account the provider's role, access level, operational criticality, data exposure, service dependency, and relevance to regulated operations.

Critical providers shall include, at minimum:

- GiG Software CoreX as core platform provider;
- GiG Software SportX as sportsbook provider;
- Alea as game aggregation provider;
- Merchant Connect as payment aggregation / gateway provider;
- AgeChecked as age-verification provider;
- Sendgrid as email / EMS provider;
- Zendesk as customer support / live chat provider; and
- any additional provider with material access to player data, compliance records, payment processes, administrative environments, credentials, logs, or security-relevant systems.

Vendor due diligence and ongoing oversight may address, as appropriate:

- legal identity, suitability, and reliability;
- scope of services and systems in use;
- categories of data processed, transmitted, supported, or accessible;
- access-control expectations and segregation principles;
- resilience, continuity, and recovery capability;
- incident notification and escalation obligations;
- logging, audit trail, and record retrievability expectations;
- confidentiality, data protection, and security commitments;
- subcontracting and dependency arrangements where relevant; and
- remediation rights, breach handling, and termination rights.

Outsourcing does not reduce the Company's responsibility. New Origin B.V. remains fully responsible for ensuring that critical outsourced providers operate in a manner consistent with the Company's legal, regulatory, operational, and security obligations.

16. Employee / Contractor Awareness, Confidentiality and Training

All relevant employees and contractors shall understand their information security responsibilities.

The Company shall provide appropriate awareness and training:

- at induction or onboarding;
- periodically thereafter, at least annually for relevant staff;
- after material regulatory, process or threat developments; and
- after major incidents or control failures where lessons learned require reinforcement.

Training shall be role-appropriate and may include confidentiality and acceptable use, password and credential hygiene, phishing and social engineering awareness, secure handling of KYC and AML records, incident reporting, access-control responsibilities, remote working expectations and vendor-security awareness.

Training records shall be retained.

17. Monitoring, Logging and Record Retention

The Company shall ensure that relevant system, administrative, security, and transactional activities are logged to the extent appropriate for security, compliance, auditability, incident investigation, and operational control.

Logs may include, as appropriate:

- user access and authentication events;
- privileged actions;
- configuration changes;
- security alerts and system events;
- transaction and payment-related records;
- KYC, AML or sanctions case-handling records where relevant; and
- complaints, responsible gaming, or other regulated case-handling records where these also support auditability and investigation.

The level, method, retention, and review of logging may vary depending on the relevant system, provider model, and operational context, provided that the resulting control environment remains appropriate to the Company's risk profile and regulatory obligations.

For Company-controlled critical administrative and security logs, review shall normally occur at least monthly and additionally following alerts, incidents, material changes, or other risk-based triggers. For vendor-managed environments, the Company shall seek review, alerting, reporting, or assurance appropriate to the provider model and criticality of the relevant service.

Logs and records shall be protected against unauthorised alteration or deletion and shall be accessible only to authorised personnel or authorised providers with a legitimate need.

18. Policy Breaches and Escalation

Failure to comply with this Policy may expose the Company to operational, regulatory, legal, financial and reputational harm.

Any actual or suspected breach of this Policy shall be escalated to the relevant manager and, where appropriate, to the Privacy & Security Owner, Compliance Officer, MLRO, COO or Managing Director depending on the nature of the matter.

Internal breaches may result in retraining, access restriction, disciplinary action or other remedial measures. Third-party breaches may result in remediation demands, heightened monitoring, suspension of access, contractual escalation or termination.

Material breaches and repeated control failures shall be documented and reviewed by management.

19. Review, Approval and Version Control

This Policy shall be reviewed at least annually and additionally when required by material business or operational changes, changes in critical vendors or outsourcing arrangements, significant incidents, audit findings, changes in payment channels or technology, or changes in legal, regulatory or licensing expectations.

The Policy owner shall coordinate review. Material updates shall be approved through the Company's internal governance process, normally by the Managing Director and with consultation of relevant control functions where the change affects compliance, payments, AML/CFT, or other regulated matters.

The current version, effective date and approval record shall be maintained in the document control section of this document.

Appendix A – Confirmed Baseline at Approval

1. Privacy & Security Owner: Raúl Moreno López, acting as internal Privacy & Security Owner within the current lean operating model.
2. Compliance Officer / MLRO at go-live: outsourced via Allyant Group B.V.; the named natural person(s) will be formally confirmed prior to go-live in line with the wider governance framework.
3. Stronger authentication and remote access baseline: multi-factor authentication shall be used wherever supported for privileged access, remote administrative access, company email, and other sensitive back-office or support environments. Administrative remote access shall use encrypted connections and approved access paths only.
4. Backup and restore baseline: critical Company-controlled data shall be backed up daily or under equivalent

provider-managed arrangements according to system criticality. Restore capability shall be tested at least semi-annually for Company-controlled critical data and otherwise through annual provider assurance, evidence, or service oversight.

5. Incident severity baseline: incidents shall be triaged according to impact on availability, Restricted data, payment integrity, regulatory exposure, fraud risk, and customer impact, using a proportionate Critical / High / Medium / Low model or equivalent internal severity record.

6. Restoration priorities: recovery efforts shall prioritise platform availability, player balances and payment-routing integrity, KYC and AML/CFT records, complaints and responsible gaming case data, and security / audit logs required for investigation, compliance, and regulatory reporting.

7. Critical vendors named from launch: GiG Software CoreX, GiG Software SportX, Alea, Merchant Connect, AgeChecked, Sendgrid, and Zendesk, together with any formally approved successor or materially equivalent provider.

Appendix B – Supporting Records Expected to Exist

The following supporting records should exist and be retrievable in order to evidence implementation of this Policy:

- information security risk assessment and risk register;
- access approval and access review records;
- joiner, mover and leaver access records;
- privileged access register;
- backup logs and restoration test records;
- incident register and post-incident review records;
- critical vendor register identifying security-relevant outsourced providers;
- vendor due diligence files and periodic oversight records;
- vendor incident escalation log;
- change approval logs and release records;
- training attendance records and awareness materials; and
- management approval record for this Policy.