



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Information Security Policy

Operator: Axum B.V.

Licence: Curaçao Gaming Authority (CGA) – Licence No. [OGL/2024/196/0574]

Effective Date: 1st April 2026

Version: 2.0 – Regulatory Alignment Update

Owner: Compliance / Information Security Function

Approved by: Board / Senior Management

Review Cycle: At least annually and upon material regulatory, operational, technology, or threat changes

Policy Statement

Axum B.V. is committed to maintaining a secure, resilient, responsible, transparent, verifiable, and reliable online gaming environment. This Information Security Policy establishes the governance, technical controls, operational requirements, monitoring obligations, and audit evidence standards used to protect player information, payment-related data, game integrity, systems, and business operations.

This policy is designed to support compliance with Curaçao gaming regulatory expectations under the National Ordinance on Games of Chance, known as the LOK, and related CGA policies and guidance. The CGA licensing framework requires online gaming operations to be safe, responsible, transparent, verifiable, and reliable, and defines “safe” as security of games, gaming equipment, and systems with adequate protection against theft, malware, and cybercrime ([CGA online gaming information](#)).

Regulatory Source Register

This policy is based on the following official or regulator-issued sources:

Source	Relevance
CGA Online Gaming Information	Licensing principles, safe/responsible/transparent/verifiable/reliable operating standard, CGA application framework



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

<u>LOK Official English Translation</u>	Operations manual, Tier-IV Curaçao data center requirement, incident reporting, reporting, inspection and enforcement powers
<u>CGA Responsible Gaming Policy</u>	Player protection controls, PAM logging, age verification, self-exclusion, cooling-off, deposit limits, RG reporting and evidence
<u>CGA AML/CFT Policy</u>	CDD, risk assessment, transaction monitoring, sanctions/PEP screening, goAML reporting, recordkeeping, independent audit
<u>CGA Complaints Policy</u>	Complaint evidence, ADR records, reporting, Responsible Gaming complaint priority, CGA access to complaint records
<u>CGA Terms and Conditions Guideline</u>	Player disclosures, T&C acceptance logging, privacy disclosures, account security, AML/RG references, chat monitoring records
<u>CGA Compliance Officer Requirements</u>	Compliance Officer independence, access to records, AML oversight, training and reporting responsibilities
<u>CGA Test Lab Certification Guideline</u>	Independent test house certification, ISO/IEC 17025 accreditation, game/RNG/RTP testing evidence

If a conflict exists between this policy and applicable law, licence conditions, CGA instructions, or official CGA portal requirements, the stricter requirement shall apply.

Purpose

The purpose of this policy is to:

- Protect information assets against unauthorized access, loss, misuse, disclosure, alteration, destruction, fraud, cyberattack, and operational disruption.
- Protect player data, player funds, player accounts, payment-related records, gaming records, audit logs, and compliance records.
- Support Axum B.V.'s obligation to provide a safe, responsible, transparent, verifiable, and reliable gaming environment.
- Maintain accurate, searchable, secure, tamper-evident, and regulator-accessible records.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Support Responsible Gaming, AML/CFT, complaints, ADR, incident reporting, and regulatory inspection readiness.
- Ensure that systems, applications, games, vendors, and operational processes are secure by design and independently reviewable.

Scope

This policy applies to:

- All Axum B.V. employees, directors, officers, contractors, consultants, temporary staff, service providers, group entities, affiliates, and third parties with access to Axum systems, data, code, infrastructure, platforms, records, or regulated operational processes.
- Production, development, test, staging, backup, and disaster recovery environments.
- Websites, mobile applications, gaming platforms, Player Account Management systems, payment systems, CRM systems, support systems, KYC/CDD systems, AML monitoring tools, Responsible Gaming tools, complaint management systems, marketing tools, reporting systems, and internal administration systems.
- Personal data, identity documents, account records, player verification records, CDD records, payment-related records, gaming transactions, financial transactions, Responsible Gaming records, complaint records, ADR records, AML/CFT records, audit logs, marketing records, support records, and compliance records.
- Cloud infrastructure, hosted infrastructure, data centers, local Curaçao infrastructure, endpoints, networks, databases, cryptographic keys, monitoring systems, supplier platforms, and any system that stores, processes, transmits, administers, or influences the confidentiality, integrity, availability, fairness, auditability, or regulatory accessibility of Axum B.V.'s licensed operations.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Information Security Objectives

Axum B.V. shall maintain an information security framework designed to:

- Protect the confidentiality of player, employee, supplier, regulatory, payment-related, and business information.
- Preserve the integrity of game systems, player accounts, transaction records, payment records, audit logs, compliance records, and regulatory reporting.
- Ensure availability, resilience, continuity, and recoverability of critical gaming services and supporting systems.
- Prevent, detect, investigate, and remediate fraud, cyber incidents, account takeover, insider misuse, unauthorized system use, and operational failures.
- Maintain accurate monitoring, audit logging, incident records, transaction reconstruction capability, and CGA inspection readiness.
- Protect payment processes, player account functions, Responsible Gaming controls, AML/CFT monitoring, complaints processes, and player protection tools.
- Maintain secure software, infrastructure, supplier, and operational processes through risk assessment, testing, certification, monitoring, and periodic independent review.

Governance and Accountability

Senior management is responsible for approving this policy, assigning accountability, allocating sufficient resources, and ensuring that information security is embedded into licensed operations. Senior management shall ensure that information security, Responsible Gaming, AML/CFT, complaints handling, player protection, regulatory reporting, and audit readiness are supported by clear ownership, adequate staffing, and documented procedures.

Day-to-day oversight may be delegated to designated control functions, including the Information Security Officer, Compliance Officer, Responsible Gaming Officer, Data Protection owner, or equivalent role. The CGA AML/CFT framework requires a designated Compliance Officer with timely



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

access to customer identification data, CDD information, transaction records, and other relevant information (CGA Compliance Officer Requirements).

The following responsibilities must be assigned and documented:

- System ownership.
- Data ownership.
- Access management.
- Privileged access review.
- Incident response and CGA incident reporting.
- Vulnerability management.
- Change management.
- Data protection and retention.
- Responsible Gaming system controls.
- AML/CFT monitoring and reporting support.
- Complaints and ADR evidence.
- Vendor and third-party oversight.
- Backup and disaster recovery.
- Business continuity.
- Audit logging and regulatory evidence production.
- Operations manual maintenance and CGA inspection readiness.

Operations Manual and Inspection Readiness

Axum B.V. shall maintain an operations manual that remains consistent with its live systems, this policy, its Responsible Gaming Policy, AML/CFT Policy, Complaints Policy, Terms and Conditions, technical architecture, and disaster recovery documentation. The LOK requires the operations manual



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

to describe games, payment possibilities, bet amounts, payouts, software, outcome-determining elements, test methods for quality monitoring, player-facing visual elements, technical measures preventing banned persons from admission, technical infrastructure, restoration possibilities for technical emergencies, and the storage of critical player, gaming transaction, and financial transaction records in a Tier-IV certified data center registered in Curaçao ([LOK Official English Translation](#)).

Axum B.V. shall be able to make the operations manual and supporting evidence available for CGA inspection within the timeframe required by law or regulator request. The LOK provides that the operations manual must be available for inspection within five working days of a CGA request ([LOK Official English Translation](#)).

Risk Management

Axum B.V. shall maintain a risk-based information security program. Information security risks must be identified, assessed, prioritized, treated, monitored, and reviewed periodically and whenever there is a material change in systems, products, payment methods, markets, suppliers, technologies, threat exposure, regulatory requirements, or control effectiveness.

Risk assessments must consider, at a minimum:

- Unauthorized access to player accounts, employee accounts, administrative systems, source code, infrastructure, and supplier systems.
- Theft, leakage, corruption, unauthorized alteration, or unauthorized deletion of personal data, CDD records, payment records, game records, transaction records, and audit logs.
- Malware, ransomware, phishing, social engineering, credential theft, and account takeover.
- Payment fraud, bonus abuse, collusion, multiple-account abuse, chargeback abuse, and suspicious transaction patterns.
- Vulnerabilities in web applications, APIs, mobile applications, gaming systems, KYC tools, payment systems, PAM systems, cloud infrastructure, and third-party components.
- Insider threats, excessive privilege, weak segregation of duties, and inadequate privileged access monitoring.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Service outages, denial-of-service attacks, data center failures, backup failure, restoration failure, and cloud service disruption.
- Weaknesses affecting game fairness, RNG/RTP integrity, outcome determinability, testing evidence, or auditability.
- Responsible Gaming control failures, including failures affecting age verification, self-exclusion, cooling-off, deposit limits, behavior tracking, and PAM logging.
- AML/CFT monitoring failures, including threshold monitoring, sanctions/PEP screening, unusual transaction detection, goAML evidence, and transaction reconstruction.
- Complaints and ADR evidence failures.

Axum B.V. shall conduct documented technology risk assessments before launching new products, new games, new payment methods, new delivery channels, new markets, new business practices, or developing technologies. The CGA AML/CFT Policy requires documented risk assessments before launching new products, business practices, delivery mechanisms, or developing technologies, with measures to mitigate identified risks (CGA AML/CFT Policy).

Asset Management

Axum B.V. shall maintain an inventory of information assets, business-critical systems, software components, databases, data stores, infrastructure components, encryption keys, administrator tools, monitoring tools, third-party integrations, and critical service providers.

Each critical asset must have:

- A documented owner.
- Classification by sensitivity and criticality.
- Processing purpose.
- Data categories processed.
- System dependencies.
- Hosting location and jurisdiction.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Backup and recovery arrangements.
- Logging and monitoring coverage.
- Regulatory evidence requirements.
- Vendor or supplier dependency, where applicable.

Unsupported software, unauthorized tools, unapproved integrations, and unapproved production changes are prohibited unless formally risk-assessed, approved, documented, and remediated within an approved timeline.

Data Classification

Information assets shall be classified according to sensitivity, business criticality, regulatory importance, and player protection impact. At minimum, the following categories are regulated or sensitive:

- Player identity data, including name, date of birth, address, nationality, identity number, verification records, and identity documents.
- CDD, EDD, sanctions, PEP, source-of-funds, source-of-wealth, and unusual transaction records.
- Player account data, login records, device data, IP addresses, account restrictions, self-exclusion status, cooling-off status, deposit limit settings, and Responsible Gaming interactions.
- Payment-related information, deposits, withdrawals, payment instruments, wallet references, chargebacks, refunds, and financial transaction records.
- Gaming records, wagers, wins, losses, bonuses, game outcomes, RNG/RTP evidence, game certificates, and transaction histories.
- Complaint, ADR, support, and regulatory correspondence records.
- Audit logs, security alerts, incident records, administrative action records, change logs, and monitoring outputs.
- Cryptographic keys, secrets, authentication credentials, API keys, service accounts, and privileged access materials.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Access Control

Access to systems and data must be granted according to least privilege, need-to-know, role-based access, segregation of duties, and regulatory function requirements. Access rights must be approved by authorized personnel, reviewed regularly, and removed promptly when no longer required.

Minimum access controls include:

- Unique user accounts for all personnel and service accounts.
- Strong password requirements and secure credential management.
- Multi-factor authentication for administrative access, remote access, critical systems, cloud consoles, source code repositories, production databases, PAM systems, payment systems, KYC/CDD systems, AML tools, and internal business systems wherever feasible.
- Segregation of duties for payments, withdrawals, bonuses, player account restrictions, AML case decisions, Responsible Gaming actions, complaint resolution, code deployment, and privileged administration.
- Privileged access controls, including documented approval, time-bounded access where feasible, enhanced logging, and periodic review.
- Immediate revocation or suspension of access following termination, role change, suspected compromise, disciplinary action, vendor termination, or regulatory concern.
- Prohibition of shared accounts unless technically necessary, formally approved, documented, tightly controlled, and logged.
- Quarterly review of access to critical systems and monthly review of privileged access unless a stricter cadence is required by risk assessment.

Compliance, AML/CFT, Responsible Gaming, complaint handling, and audit functions must receive timely access to the records necessary to perform their duties without receiving unnecessary administrative privileges. The Compliance Officer must have timely access to customer identification data, CDD information, transaction records, and other relevant information needed for statutory AML/CFT responsibilities (CGA Compliance Officer Requirements).



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Authentication and Customer Account Security

Player-facing systems must include controls to reduce unauthorized access, account takeover, identity fraud, multiple-account abuse, payment fraud, and prohibited participation.

Customer account controls shall include:

- Strong password standards.
- Secure credential storage.
- Session management controls.
- Login monitoring.
- Device, IP, and location anomaly detection where feasible.
- Fraud and multiple-account detection.
- Secure password reset and account recovery procedures.
- Controls preventing unauthorized changes to personal details, payment instruments, limits, exclusions, and security settings.
- Controls to detect and respond to credential stuffing, brute force attacks, suspicious login behavior, and account takeover.

Players must be informed through the Terms and Conditions that they are responsible for keeping login credentials secure, and the Terms and Conditions must address liability for unauthorized access to player accounts. The CGA Terms and Conditions guideline requires account security provisions and player disclosure of liability for unauthorized account access ([CGA Terms and Conditions Guideline](#)).

Age Verification and Prohibited Participation Controls

Axum B.V. shall maintain technical and operational controls to prevent minors, self-excluded players, banned persons, duplicate accounts created to evade restrictions, and other prohibited persons from participating in games of chance.

Minimum controls include:



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Date-of-birth capture at registration.
- Player confirmation that the player is at least 18 years old.
- Government-issued ID verification where required by law, policy, risk trigger, threshold, or prior to first withdrawal.
- Additional verification where risk indicators exist, such as electronic verification, payment validation, third-party database checks, or selfie verification.
- Immediate closure of accounts identified as belonging to minors.
- Deposit refund and winnings treatment processes consistent with law, policy, and legal advice.
- Records of all age-verification processes, outcomes, failures, closures, and communications.

The CGA Responsible Gaming Policy prohibits persons under 18 from participating in games of chance and requires records of age-verification processes and outcomes for regulatory review ([CGA Responsible Gaming Policy](#)).

Responsible Gaming System Controls

Axum B.V. shall maintain Responsible Gaming controls that are embedded into player account systems, PAM workflows, support operations, marketing systems, and compliance reporting.

Responsible Gaming controls must include:

- A designated Responsible Gaming role or assigned Compliance Officer responsibility.
- Annual management reporting on Responsible Gaming policy and procedure effectiveness.
- Reporting of material Responsible Gaming policy changes to the CGA.
- Website and application access to Responsible Gaming information and tools.
- Self-assessment tools.
- Cooling-off options.
- Self-exclusion options.
- Deposit limits on a daily, weekly, or monthly basis.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Time, loss, wager, or reality-check controls where required by risk profile or policy.
- Monitoring of player behavior indicators.
- Escalation of concerning behavior to trained personnel.
- Documentation of player and operator-initiated Responsible Gaming interactions in the PAM system.

The CGA Responsible Gaming Policy requires all player or operator-initiated Responsible Gaming interactions to be recorded in the PAM system, including indicators of concern and actions taken (CGA Responsible Gaming Policy).

Self-Exclusion and Cooling-Off

Axum B.V. shall implement self-exclusion and cooling-off controls that are technically enforceable and auditable.

Minimum controls include:

- Cooling-off periods activated through self-service or manual support channels within required timelines.
- Self-exclusion for at least one year and longer options where offered.
- Irreversible self-exclusion for the selected period.
- No wagering and no deposits during self-exclusion.
- Blocking across all brands, domains, and applications under the licence where required.
- Duplicate-account detection for self-excluded players.
- Payment method blocking where possible.
- Marketing suppression for self-excluded players.
- Logs of activation, confirmation, duration, scope, affected domains, payment methods, staff involvement, and reactivation requests.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

The CGA Responsible Gaming Policy requires self-exclusion to block all verticals, prevent deposits and wagering, apply across all brands/domains under the license, identify duplicate accounts, and block marketing messages ([CGA Responsible Gaming Policy](#)).

Deposit Limits and Player Account History

Axum B.V. shall offer mandatory deposit limit controls and ensure they are technically enforced.

Minimum controls include:

- Daily, weekly, or monthly deposit limit options.
- Immediate effect for more restrictive limit changes.
- A 24-hour waiting period for less restrictive limit changes.
- Automated prevention of deposits that exceed active limits.
- Audit logs for limit creation, limit changes, failed limit breaches, staff actions, and system overrides.

Players must be able to access at least the last six months of betting or wagering history with timestamps. Requests for longer periods must be fulfilled within 10 working days unless an extension is permitted by the CGA. The CGA Responsible Gaming Policy requires access to at least six months of betting or wagering history and a 10-working-day response period for longer-period requests ([CGA Responsible Gaming Policy](#)).

Behavior Tracking and Intervention

Axum B.V. shall maintain processes and tooling to detect potential gambling harm and escalate concerns.

Monitoring indicators shall include, as applicable:

- Sudden unexplained increases in wagering or gaming session patterns.
- Repeated failed transactions due to insufficient funds.
- Repeated reversal of withdrawals.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Inexplicably extended play sessions.
- Increased or agitated communication with support.
- Frequent changes to limits, cooling-off, or other Responsible Gaming tools.
- Maxing out credit cards or similar financial distress indicators where visible.
- Attempts to open multiple accounts.

When concerning indicators are detected, Axum B.V. may apply interventions including staff outreach, Responsible Gaming messaging, mandatory limits, temporary suspension, cooling-off, self-exclusion suggestions, or operator-initiated exclusion. All indicators, decisions, and actions must be logged in the PAM system.

AML/CFT Monitoring and System Controls

This policy supports but does not replace Axum B.V.'s AML/CFT Policy. Security, data, access, logging, and monitoring systems must support AML/CFT compliance.

Axum B.V. shall maintain system controls for:

- Customer identification and verification.
- Customer due diligence at applicable thresholds.
- Enhanced due diligence where required by risk.
- Customer risk assessment.
- Business risk assessment evidence.
- Sanctions and PEP screening.
- Transaction monitoring.
- Unusual transaction case management.
- goAML reporting evidence.
- Anti-tipping-off access restrictions.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- CDD and transaction record retention.
- Account restrictions and freezes where required.

The CGA AML/CFT Policy requires CDD measures when players engage in financial transactions equal to or above NAf. 4,000, including linked transactions meeting the threshold, and requires transaction records sufficient to reconstruct individual transactions ([CGA AML/CFT Policy](#)).

If a CDD threshold is reached, Axum B.V. shall apply account controls in accordance with AML/CFT procedures. If required information is not received within 30 days of reaching the threshold, Axum B.V. shall follow the relationship termination and funds handling requirements set out in the AML/CFT Policy and applicable law. The CGA AML/CFT Policy includes account restriction and termination requirements connected to the NAf. 4,000 CDD threshold ([CGA AML/CFT Policy](#)).

Sanctions, PEP, and Source-of-Funds Controls

Axum B.V. shall maintain sanctions and PEP screening controls proportionate to risk and regulatory obligations.

Minimum controls include:

- Screening against UN, EU, local Curaçao, and other required sanctions lists.
- PEP screening at onboarding and periodically during the relationship.
- Positive match investigation workflow.
- Senior management or Compliance Manager approval where required.
- Source-of-funds and source-of-wealth review for applicable high-risk players and PEPs.
- Enhanced monitoring of high-risk players.
- Audit trails for screening, match resolution, approvals, and decisions.

The CGA AML/CFT Policy requires sanctions screening, PEP identification, senior approval for PEP relationships, source-of-wealth/source-of-funds checks, and enhanced ongoing monitoring ([CGA AML/CFT Policy](#)).



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Data Protection and Privacy

Personal data and protected information must be processed lawfully, fairly, transparently, securely, and only for legitimate business, contractual, regulatory, player protection, fraud prevention, AML/CFT, and compliance purposes.

Axum B.V. shall:

- Restrict personal data access to authorized users and systems.
- Protect sensitive data through secure transmission, secure storage, access control, monitoring, and retention controls.
- Maintain data processing records and privacy notices appropriate to the operation.
- Disclose to players how personal data is collected, used, stored, retained, shared, monitored, and protected.
- Ensure that player data disclosures in Terms and Conditions and Privacy Policy cover collection, use, storage, retention, sharing, AML/CFT monitoring, sanctions/PEP screening, Responsible Gaming monitoring, complaint handling, and regulatory reporting.

The CGA Terms and Conditions guideline requires disclosure of how player data is processed and retained, and states that the policy must cover collection, use, storage, retention, and sharing of personal data ([CGA Terms and Conditions Guideline](#)).

Data Storage, Curaçao Hosting, and Regulatory Access

Axum B.V. shall maintain digital records of critical player information, gaming transactions, and financial transactions in a manner that is accurate, searchable, secure, tamper-evident, resilient, and available for regulatory review.

The LOK requires critical digital records relating to players, gaming transactions, and financial transactions to be stored on a server of a Tier-IV certified data center registered in Curaçao and available to the CGA at all times ([LOK Official English Translation](#)).

Axum B.V. shall maintain evidence of:



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Curaçao data center provider.
- Tier-IV certification or equivalent regulator-accepted evidence.
- Server location and hosting contract.
- Data categories stored on the Curaçao server.
- Data synchronization, replication, or mirroring design.
- Encryption at rest and in transit.
- Backup and recovery arrangements.
- Regulatory access procedure.
- Monthly availability testing of critical records.
- Incident response procedure for data unavailability.

Recordkeeping and Retention

Axum B.V. shall maintain a record retention schedule by record class. Records must be retained for at least the period required by law, CGA policy, licence condition, contractual obligation, litigation hold, regulatory inquiry, or business need.

The following minimum retention requirements apply unless a longer period is required:

Record Class	Minimum Retention
AML/CFT transaction records	At least 5 years
CDD and identity verification records	At least 5 years after the business relationship ends or after the occasional transaction
Account files and business correspondence relevant to CDD	At least 5 years
Unusual transaction records and decisions not to report	At least 5 years
Frozen account records	At least 5 years



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Business Risk Assessment and Customer Risk Assessment records	At least 5 years
AML/CFT training records	At least 5 years or longer if required by law or policy
Independent AML/CFT audit reports	At least 5 years
Operator-initiated Responsible Gaming exclusion records	At least 5 years
Responsible Gaming PAM logs	At least 5 years unless a longer period is required
Complaint records unresolved, escalated to ADR, or subject to legal proceedings	Lesser of 5 years or the period required by data protection, statute of limitations, or other applicable law/guideline, unless legal hold requires longer
T&C versions and player acceptance logs	From 24 December 2024 onward, or longer if required
Security incident records	At least 5 years unless legal or regulatory needs require longer
Critical audit logs	At least 5 years unless a shorter period is approved for low-risk logs and not prohibited by law

The CGA AML/CFT Policy requires transaction and CDD records to be retained for at least five years, and the CGA Responsible Gaming Policy requires operator-initiated exclusion records to be kept for at least five years ([CGA AML/CFT Policy](#), [CGA Responsible Gaming Policy](#)).

Historical records must not be altered, deleted, anonymized, or purged except under approved retention procedures, legal requirements, documented data protection rules, and applicable regulatory permissions. All deletion or alteration of regulated records must be logged.

Audit Logging and Monitoring

Axum B.V. shall maintain centralized, secure, tamper-evident audit logging for critical systems and regulated workflows.

Audit logs must be enabled for:

- Authentication and failed authentication.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Privileged access and administrative actions.
- Access to sensitive personal data, CDD records, payment records, and transaction records.
- Player registration, verification, KYC/CDD status changes, and account closure.
- Player account changes, including email, phone, address, payment method, password, MFA, and security settings.
- Self-exclusion, cooling-off, limits, Responsible Gaming interactions, and operator-initiated restrictions.
- Deposits, withdrawals, wagers, wins, losses, bonuses, refunds, chargebacks, adjustments, and wallet movements.
- AML/CFT monitoring alerts, sanctions/PEP screening results, unusual transaction cases, account freezes, and goAML reporting milestones.
- Complaint intake, categorization, evidence, response, escalation, ADR referral, and legal-action status.
- Terms and Conditions acceptance, non-acceptance, material-change re-acceptance, and notification evidence.
- Chat, messaging, and support interactions where required for fraud, collusion, Responsible Gaming, complaints, or AML/CFT monitoring.
- System configuration changes.
- Code deployment, release approval, emergency changes, and rollback.
- Game configuration, RNG/RTP certificate updates, and game enablement or disablement.
- Security alerts, vulnerability remediation, incident investigation, and evidence handling.

Each log entry must capture, where applicable:

- Timestamp in UTC.
- User, staff, admin, service, or player identifier.
- Role or permission level.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Session ID.
- IP address.
- Device or browser identifier.
- Event type.
- System or component.
- Before-and-after values for changes.
- Transaction or case identifier.
- Payment instrument reference or privacy-preserving unique identifier where applicable.
- Approval reference.
- Outcome.
- Failure reason.
- Source system.

Logs must be protected from unauthorized access, alteration, deletion, and tampering. Critical logs shall be centralized and retained according to the retention schedule. Critical alerts must be reviewed daily, privileged activity reviewed at least monthly, and regulated evidence samples reviewed at least quarterly.

Player Transaction Records and Reporting Support

Axum B.V. shall maintain transaction records sufficient to reconstruct player account activity, financial transactions, gaming activity, and regulatory reports.

Player transaction records must include, where applicable:

- Player account identifier.
- Domain, brand, application, or vertical.
- Date and time.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Transaction type.
- Amount and currency.
- Deposit, withdrawal, wager, win, loss, bonus, refund, chargeback, adjustment, or wallet movement classification.
- Payment instrument type.
- Privacy-preserving unique payment account identifier.
- Transaction status.
- Processor or wallet reference.
- AML/CFT monitoring status.
- Responsible Gaming impact where applicable.
- Reconciliation status.

The LOK provides that transaction reports include total amounts credited or debited, the nature of account crediting or debiting, payment instrument type, and a unique payment-account identifier not directly traceable to the player's identity (LOK Official English Translation).

Cryptography and Key Management

Appropriate encryption or equivalent protective controls must be used to safeguard sensitive data in transit and at rest, including player information, identity documents, payment-related data, authentication credentials, backups, regulatory reports, audit logs, administrative connections, and data transfers to or from third parties.

Cryptographic keys must be:

- Securely generated.
- Stored in approved key management systems or hardware security modules where appropriate.
- Restricted to authorized roles.
- Rotated according to risk and policy.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Revoked or retired when compromised, expired, or no longer required.
- Protected from unauthorized export or disclosure.
- Logged when accessed, used, rotated, or revoked.

Weak, deprecated, or insecure cryptographic protocols and ciphers must not be used in production systems where stronger approved alternatives are available.

Secure Development and Change Management

Security must be integrated into the software development lifecycle for websites, mobile applications, gaming systems, APIs, internal platforms, PAM workflows, KYC/CDD systems, payment integrations, AML monitoring, Responsible Gaming tooling, and reporting systems.

Minimum secure development controls include:

- Secure design review.
- Code review.
- Dependency scanning.
- Static and dynamic application security testing where appropriate.
- Secrets scanning.
- Vulnerability remediation.
- Controlled deployment.
- Separation of development, test, staging, and production environments.
- Change approval and rollback plans.
- Testing before production release.
- Emergency change logging and retrospective review.
- Regulatory impact assessment for changes affecting operations manual content, player data, payments, AML/CFT, Responsible Gaming, complaints, audit logs, or reporting.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

All material system changes must be documented, reviewed, approved, tested, and implemented through the change management process. Changes to the operations manual must be tracked and reported where required. The LOK requires amendment reports twice per year by June 15 and January 15 detailing changes to the operations manual ([LOK Official English Translation](#)).

Game Integrity, Certification, and Technical Assurance

Axum B.V. shall ensure that games owned, operated, or controlled by it are independently tested and certified where required. Technical controls must preserve game integrity, fairness, auditability, outcome determinability, and player trust.

Axum B.V. shall maintain:

- Game inventory.
- RNG certificates.
- RTP certificates.
- Test lab reports.
- Release and version history.
- Game configuration change logs.
- Approval evidence for new games or game replacements.
- Evidence that applicable independent testing providers meet CGA expectations.

The CGA Test Lab Certification guideline recognizes ISO/IEC 17025-accredited testing against technical standards applicable to online gaming systems, RNGs, game fairness, RTP calculations, and other components required for compliance verification ([CGA Test Lab Certification Guideline](#)).

Vulnerability Management and Security Testing

Axum B.V. shall maintain procedures to identify, assess, remediate, and track vulnerabilities affecting internal systems, player-facing systems, cloud infrastructure, third-party components, APIs, mobile applications, payment integrations, KYC tools, PAM systems, and administrative systems.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Security testing should include, as appropriate:

- Vulnerability scanning.
- Penetration testing.
- Configuration reviews.
- Access control reviews.
- Application security testing.
- API security testing.
- Cloud security reviews.
- Recovery testing.
- Logging and monitoring tests.
- Transaction reconstruction tests.
- Responsible Gaming control tests.
- AML/CFT monitoring system tests.
- Periodic independent audits where required.

Vulnerabilities must be risk-ranked and remediated within defined timelines. Exceptions must be documented, risk-accepted by authorized management, time-bound, and periodically reviewed.

Network and Infrastructure Security

Critical systems must be hosted, administered, segmented, monitored, and protected in a manner that supports confidentiality, integrity, availability, resilience, traceability, and regulatory access.

Network and infrastructure controls may include:

- Firewalls and network segmentation.
- Intrusion detection or prevention.
- Secure remote access.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Endpoint detection and response.
- Anti-malware controls.
- Secure configuration baselines.
- Patch management.
- DDoS protection.
- Cloud security monitoring.
- Privileged access workstations for administrators where appropriate.
- Continuous monitoring of critical systems.

Administrative interfaces and critical infrastructure must not be exposed unnecessarily to the public internet. Remote administration must be restricted, secured with MFA, logged, monitored, and periodically reviewed.

Third-Party Risk Management

All third parties with access to Axum systems, data, infrastructure, code, administrative tools, payment functions, KYC/CDD workflows, AML/CFT monitoring, Responsible Gaming processes, complaint handling, marketing systems, or operational processes must be subject to risk-based due diligence and contractual security requirements.

Covered third parties include:

- Hosting providers.
- Cloud providers.
- Game providers.
- Software suppliers.
- Managed service providers.
- KYC/CDD providers.
- AML screening providers.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Payment processors.
- Wallet providers.
- Customer support vendors.
- Marketing technology vendors.
- Affiliates and marketing partners.
- Group entities and other outsourced service providers.

Contracts should require third parties to:

- Maintain appropriate security controls.
- Protect personal data and regulated records.
- Cooperate with audits, evidence requests, and regulatory inquiries.
- Notify Axum B.V. of security incidents without undue delay.
- Support retention, access, and retrieval of regulated records.
- Comply with applicable law, CGA expectations, and Axum B.V. policies.
- Return or securely delete data at termination subject to legal and regulatory retention requirements.

Where Axum B.V. relies on third parties for CDD information, Axum B.V. must obtain required identification information immediately, maintain written arrangements ensuring documentation is available upon request, periodically test the arrangement, and ensure the third party is regulated, supervised, and has CDD and recordkeeping measures in place. The CGA AML/CFT Policy states that the decision to onboard or continue a customer relationship on the basis of risk cannot be outsourced and that ultimate responsibility remains with the casino ([CGA AML/CFT Policy](#)).

Monitoring and Incident Management

Axum B.V. shall maintain monitoring capabilities sufficient to detect anomalous activity, security events, attempted compromise, account takeover, fraud indicators, AML/CFT alerts, Responsible Gaming indicators, payment anomalies, operational failures, and game integrity concerns.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Axum B.V. shall maintain a documented incident response process to:

- Identify incidents.
- Classify severity and regulatory reportability.
- Contain incidents.
- Preserve evidence.
- Investigate root cause.
- Remediate vulnerabilities.
- Communicate internally and externally.
- Notify affected parties where required.
- Report to regulators or authorities where required.
- Document lessons learned and corrective actions.

CGA Incident Reporting

Axum B.V. shall assess all security, operational, fraud, software, game integrity, and player protection incidents against Curaçao reporting requirements.

Any incident involving a security breach compromising personal information or game details, failure, loss, or damage to equipment or software causing loss of games, attempted fraud or criminal behavior by players, or any event threatening responsible or reliable operation or public trust must be escalated immediately and reported to the CGA within 24 hours where required. The LOK requires incident reports within 24 hours for these categories (LOK Official English Translation).

Incident records must include:

- Incident category.
- Date and time detected.
- Date and time occurred, if known.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Reporting deadline assessment.
- Systems affected.
- Data affected.
- Players affected.
- Game integrity impact.
- Payment or transaction impact.
- Responsible Gaming impact.
- AML/CFT impact.
- Containment actions.
- Corrective actions.
- Root cause.
- Evidence preserved.
- Internal escalations.
- External reports.
- Customer communications.
- Regulator communications.
- Lessons learned.

Complaints and ADR Evidence

This policy supports Axum B.V.'s Complaints Policy and ADR obligations. Systems and records must support fair, accessible, timely, evidence-based, and regulator-reviewable complaint handling.

Complaint records must include:

- Player name and account identifier.
- Date of complaint.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Date of disputed event.
- Complaint category.
- Description of disputed conduct.
- Supporting documentation.
- Responsible handler.
- Responsible Gaming priority flag, where applicable.
- AI involvement flag, where applicable.
- Human review evidence for Responsible Gaming and complex complaints.
- Response deadlines.
- Final determination.
- Evidence supporting the decision.
- ADR referral status.
- Legal action status.
- CGA reporting classification.

The CGA Complaints Policy requires priority handling for Responsible Gaming complaints, human handling for Responsible Gaming and complex complaints, twice-yearly reporting to the CGA, and CGA access to complaint and dispute records at any time ([CGA Complaints Policy](#)).

Terms and Conditions Evidence

Axum B.V. shall maintain evidence that players received, reviewed, and accepted the applicable Terms and Conditions.

Controls must include:

- Current T&C availability within one click from the player account area.
- Historical archive of T&C versions from 24 December 2024 onward.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Secure logs of player acceptance or non-acceptance.
- Active acknowledgement at registration.
- Active re-acceptance for material changes.
- Evidence of player notification of changes.
- Version ID, language, timestamp, IP/device, player ID, action, and notification method.

The CGA Terms and Conditions guideline requires licensees to maintain historical T&C archives, securely log player acceptance or non-acceptance, retain notification evidence, and make evidence available to the CGA upon request ([CGA Terms and Conditions Guideline](#)).

Chat, Messaging, and Support Monitoring

Axum B.V. shall monitor, log, and review chat, messaging, and support interactions where necessary to detect fraud, collusion, abusive behavior, Responsible Gaming concerns, AML/CFT concerns, complaint issues, or regulatory risks.

Monitoring must be:

- Disclosed to players through appropriate notices.
- Limited to legitimate business, security, compliance, and player protection purposes.
- Restricted to authorized reviewers.
- Logged and auditable.
- Retained according to the retention schedule.

The CGA Terms and Conditions guideline requires controls for monitoring, logging, and recording chat and message activity to detect collusion or fraud ([CGA Terms and Conditions Guideline](#)).

Business Continuity and Disaster Recovery

Axum B.V. shall maintain documented business continuity and disaster recovery arrangements for critical services, systems, and data.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

These arrangements must support recovery from:

- Cyber incidents.
- Ransomware.
- Account takeover campaigns.
- Payment system failure.
- Gaming platform failure.
- Hosting or data center failure.
- Data corruption.
- Backup failure.
- Cloud service outage.
- Denial-of-service attack.
- Critical supplier failure.
- Regulatory data access disruption.

At minimum, Axum B.V. shall:

- Maintain secure backups of critical systems and data.
- Protect backups from unauthorized access, alteration, deletion, and ransomware impact.
- Define recovery time objectives and recovery point objectives for critical systems.
- Test restoration and continuity procedures periodically.
- Document fallback, escalation, and communication procedures.
- Verify that critical player, gaming transaction, and financial transaction records remain available for regulatory review.
- Include restoration possibilities for technical emergencies in the operations manual.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Physical and Environmental Security

Where Axum B.V. controls offices, equipment rooms, endpoint storage, local infrastructure, or regulated records, physical security controls must protect against unauthorized access, theft, damage, tampering, and service disruption.

Controls may include:

- Badge access.
- Visitor logging.
- CCTV where lawful.
- Secure device storage.
- Clear desk expectations for sensitive materials.
- Secure disposal.
- Environmental protections.
- Access review for restricted areas.

Where third-party data centers or cloud providers are used, Axum B.V. must obtain and maintain evidence that the provider maintains physical and environmental security appropriate to the criticality of hosted systems and regulatory recordkeeping.

Security Awareness and Training

All relevant personnel must receive information security awareness training at induction and at regular intervals thereafter. Training must be proportionate to role and risk.

Training shall cover, as applicable:

- Password and authentication hygiene.
- Phishing and social engineering.
- Data handling and confidentiality.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Incident reporting obligations.
- Secure use of systems and devices.
- Privileged access expectations.
- Responsible Gaming indicators and escalation.
- AML/CFT red flags and reporting.
- Complaint and ADR evidence handling.
- Secure handling of identity documents and payment-related data.
- Third-party and remote access responsibilities.

Training records must include training content, staff names, dates, completion status, test results where used, and the ongoing training plan. The CGA AML/CFT Policy requires records of training content, names, dates, test results, and an ongoing training plan, and the CGA Responsible Gaming Policy requires training for customer support, VIP, and marketing staff ([CGA AML/CFT Policy](#), [CGA Responsible Gaming Policy](#)).

Independent Audit, Review, and Evidence Pack

Axum B.V. shall maintain an audit-ready evidence pack demonstrating implementation of this policy and related regulatory controls.

The evidence pack shall include:

- Approved policy versions.
- Regulatory source register.
- Operations manual and crosswalk.
- Risk assessments.
- Asset inventory.
- Access reviews.
- Privileged access logs.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

- Security monitoring reports.
- Incident register.
- CGA incident reporting records.
- Vulnerability scans and remediation records.
- Penetration test reports.
- Backup and restoration test records.
- Tier-IV Curaçao data center evidence.
- PAM Responsible Gaming logs.
- Self-exclusion, cooling-off, and deposit limit test evidence.
- AML/CFT monitoring and screening evidence.
- goAML reporting records.
- Complaint and ADR registers.
- T&C acceptance logs and historical archives.
- Training records.
- Vendor due diligence and contract evidence.
- Game/RNG/RTP certificates.
- Independent audit reports.

The CGA AML/CFT Policy requires an annual independent audit that includes review of AML/CFT manuals, risk assessments, compliance management, transaction testing, training adequacy, electronic monitoring systems, unusual transaction sampling, and record retention systems (CGA AML/CFT Policy).

Regulatory Reporting Calendar

Axum B.V. shall maintain a reporting calendar covering regulatory, AML/CFT, Responsible Gaming, complaint, operations manual, and incident reporting obligations.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

At minimum, the calendar shall track:

Report / Event	Timing
CGA incident reports	Within 24 hours where reportable under LOK
Operations manual amendment reports	June 15 and January 15
Complaint reports to CGA	January 15 and June 15
Annual financial statements	June 30 of the following year, where applicable
Responsible Gaming management effectiveness report	At least once every 12 months
Independent AML/CFT audit	At least annually
Business Risk Assessment review	At least annually and upon trigger events
Access reviews	Quarterly, or more frequently for privileged access
Privileged access review	Monthly or risk-based
Backup restoration test	Periodically according to system criticality
Security policy review	At least annually and upon material change

The LOK requires incident reports within 24 hours and operations manual amendment reports twice yearly by June 15 and January 15, while the CGA Complaints Policy requires twice-yearly complaint reports to the CGA ([LOK Official English Translation](#), [CGA Complaints Policy](#)).

Policy Exceptions and Breaches

Any exception to this policy must be documented, risk-assessed, approved by authorized management, assigned an owner, limited in scope, time-bound, and reviewed periodically.

Exceptions may not be used to bypass legal, regulatory, licence, player protection, AML/CFT, Responsible Gaming, or CGA reporting obligations unless approved by legal counsel and permitted by applicable law or regulator instruction.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Violations of this policy may result in disciplinary action, suspension of access, contractual remedies, regulator reporting, legal action, or termination of service provider arrangements, depending on the nature and severity of the breach.

Review and Maintenance

This policy must be reviewed at least annually and also when there are material changes to:

- CGA or Curaçao regulatory requirements.
- Licence conditions.
- Business operations.
- Games or products.
- Payment methods.
- Markets or jurisdictions.
- Technology architecture.
- Data center or hosting arrangements.
- Supplier arrangements.
- Threat landscape.
- Incident trends.
- Audit findings.
- Control effectiveness.

Updated versions must be approved by management and communicated to relevant stakeholders.

Associated procedures, standards, evidence records, and system configurations must be maintained to demonstrate implementation and readiness for internal review, external audit, and CGA inspection.



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Appendix A: Minimum Audit Log Events

Category	Events
Authentication	Login, failed login, MFA challenge, MFA reset, password reset, session creation, session termination
Privileged Access	Admin login, role assignment, privilege elevation, production access, database query, configuration change
Player Account	Registration, profile update, payment method change, account closure, duplicate account flag, account lock
KYC/CDD	ID upload, verification result, threshold trigger, CDD completion, EDD review, document expiry, CDD failure
AML/CFT	Sanctions result, PEP result, unusual activity alert, case decision, freeze, unfreeze, goAML report milestone
Payments	Deposit, withdrawal, refund, chargeback, wallet movement, payment failure, payment reversal
Gaming	Wager, win, loss, bonus, adjustment, game launch, game outcome, game error, interrupted play
Responsible Gaming	Self-exclusion, cooling-off, deposit limit, limit change, RG contact, behavior flag, intervention, operator exclusion
Complaints	Complaint received, category assigned, evidence added, response sent, ADR referral, final determination
T&C	Version displayed, acceptance, non-acceptance, material-change notice, re-acceptance
Security	Alert, vulnerability, patch, incident, containment, evidence export, forensic action
Change Management	Change request, approval, deployment, rollback, emergency change, retrospective review

Appendix B: Key Evidence Owners

Evidence Area	Owner
Policy approval and regulatory source register	Compliance



Project: Information Security Policy	Axum BV
Date: 1 st April 2026	

Operations manual	Compliance and Product
Security controls and audit logs	Information Security
Tier-IV Curaçao data center evidence	Technology
Game certification and testing evidence	Product and Compliance
Responsible Gaming logs and reporting	Responsible Gaming Officer
AML/CFT monitoring and reporting	Compliance Officer
Complaint and ADR records	Customer Support and Compliance
Vendor due diligence	Vendor Management
Training records	HR and Compliance
Independent audit reports	Board, Compliance, and Internal Audit