

Operational Manual
Esti Technologies N.V.

Address: Schottegatweg Oost 10 Unit 1-9,
Bon Bini Business Center, Curaçao

Version: 1.0 | Effective date: 2025-08-28

This document defines the governance model, core processes, policies and controls of Esti Technologies N.V. for operating online gaming services under a Curaçao licence.

Document Control

Field	Value
Document Title	Operational Manual – Esti Technologies N.V.
Owner	Compliance Officer
Approver	Chief Executive Officer (CEO)
Version	1.0
Effective Date	2025-08-28
Review Cycle	At least annually, or upon material change
Confidentiality	Internal – Do not distribute externally without approval

Table of Contents

Note: Update the Table of Contents in Word (References → Table of Contents) after opening the document.

1. 1. Mission, Vision & Values
2. 2. Organizational Structure
3. 3. Roles & Responsibilities
4. 4. Core Business Processes
5. 5. Governance & Control
6. 6. Policies & Procedures
7. 7. Systems & Tools
8. 8. Reporting & Communication
9. 9. Security & Compliance
10. 10. Appendices

1. Mission, Vision & Values

Mission

To operate a safe, fair, and entertaining online gaming business that complies with Curaçao regulations, protects players, and delivers sustainable growth.

Vision

To become a trusted iGaming operator recognized for responsible conduct, operational excellence, and data-driven decision-making.

Values

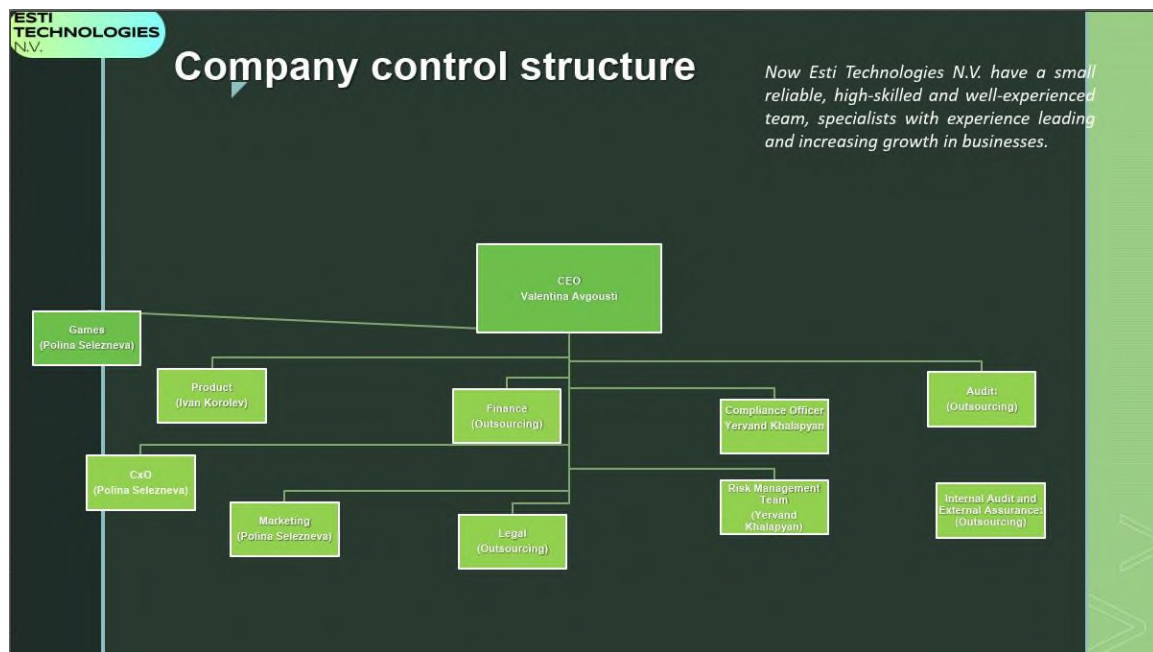
- Integrity & Compliance – we meet and exceed regulatory expectations.
- Player First – safety, fairness, and transparency guide all decisions.
- Operational Excellence – standardized, auditable, and efficient processes.
- Data-Driven – measurable KPIs and continuous improvement.
- Accountability – clear ownership via RACI and strong governance.

2. Organizational Structure

Esti Technologies N.V. operates with a lean core team supported by specialist outsourcing partners. The CEO provides overall leadership; the Compliance Officer ensures adherence to laws, licence conditions and internal policies; the Risk Management Team monitors fraud and responsible gaming risks. Finance, Legal, and Audit functions are outsourced to qualified providers with formal SLAs.

- CEO – Valentina Avgousti
- Compliance Officer – Yervand Khalapyan
- Risk Management Team – Led by Yervand Khalapyan
- Games – Polina Selezneva
- Product – Ivan Korolev
- CxO / Operations – Polina Selezneva
- Marketing – Polina Selezneva
- Finance – Outsourcing
- Legal – Outsourcing
- Audit – Outsourcing (incl. Internal Audit & External Assurance)

Organizational Chart:



3. Roles & Responsibilities

Clear accountability is maintained through a RACI model (Responsible, Accountable, Consulted, Informed).

[illegible]

& taxes

Complaints & disputes	I	A/R	C	I	I	I	I	C	I
--------------------------	---	-----	---	---	---	---	---	---	---

Business continuity & incidents	A	R	R	I	R	I	C	C	C
---------------------------------------	---	---	---	---	---	---	---	---	---

4. Core Business Processes

4.1 Player Lifecycle

11. Registration – collect identity data and consent; verify age and jurisdiction eligibility.
12. KYC/AML – risk-based identity verification using approved providers; PEP/sanctions screening; source of funds where required.
13. Deposits – accept payments only via approved PSPs; monitor velocity and anomalies.
14. Gameplay – ensure fair game configurations, RTP settings per vendor, and session controls.
15. RG Controls – limits (deposit, loss, reality checks), self-exclusion, cool-off; monitor behavioural markers of harm.
16. Withdrawals – process only to verified payment methods; apply anti-fraud checks; record approval trail.
17. Complaints & Disputes – follow documented resolution workflow; escalate to ADR where applicable.
18. Account Closure & Data Retention – apply retention schedule and GDPR-aligned rights where applicable.

4.2 Payments & Treasury

- PSPs and acquiring banks onboarded via due diligence and signed SLAs.
- Daily reconciliation between platform balances, PSP reports, and bank statements.
- Segregation of player funds according to internal policy; restricted access to payment credentials.
- Chargeback handling with evidence packs and root-cause analysis.

4.3 Games & Content Management

- Vendor onboarding checklists (licence, RTP certificates, jurisdictional availability).
- Game configuration approvals and release notes; version tracking.
- Monthly review of top/bottom performers; responsible content flags.

4.4 Risk, Fraud & Monitoring

- Real-time risk rules (multi-accounting, device fingerprinting, velocity).
- Post-event analytics; suspicious activity reports (SAR) to the authority as required.
- Quarterly risk assessment covering AML/CFT, RG, cybersecurity, and operational risk.

4.5 Change Management

19. Submit Change Request (CR) with impact assessment and rollback plan.
20. Approval by Product (functional), Compliance (regulatory), and CEO (material changes).
21. Staging/UAT with test evidence; deployment window; post-release review.
22. Versioning and documentation in the release log.

4.6 Incident Management

23. Detect – monitoring alerts or user reports (ticketing system).

24. Triage – classify severity (SEV1–SEV3) and assemble response team.
25. Contain/Remediate – implement fixes; communicate status to stakeholders.
26. Report – incident report within 24–72h depending on severity; notify authority and users if required.
27. Learn – root-cause analysis and corrective actions tracked to closure.

4.7 Vendor & Outsourcing Management

- Due diligence (licence, security posture, financial stability).
- Contract with clear KPIs, SLAs, data-processing terms, and audit rights.
- Performance reviews at least quarterly; risk re-assessment annually.

5. Governance & Control

- Three Lines of Defense – Operations (1st), Compliance/Risk (2nd), Independent Audit (3rd).
- Board/CEO oversight with monthly KPI pack and risk dashboard.
- Policy Management – controlled repository; approval by CEO; annual review.
- Business Continuity & Disaster Recovery – defined RTO/RPO; tested at least annually.
- Outsourcing Oversight – SLAs, reporting cadence, escalation paths, and exit plans.

6. Policies & Procedures

- AML/CFT & Sanctions Screening Policy
- KYC & Player Due Diligence Procedure
- Responsible Gaming Policy
- Privacy & Data Protection (incl. data subject rights, retention schedule)
- IT Security & Access Control Policy
- Fair Gaming & RTP Control Policy
- Complaints & Dispute Resolution Procedure
- Marketing & Advertising Compliance (jurisdictional restrictions)
- Anti-Bribery, Gifts & Conflicts of Interest Policy
- Whistleblowing Policy
- HR & Training Policy (including onboarding and annual refreshers)

7. Systems & Tools

- Platform: proprietary iGaming platform with integrations to game aggregators.
- Hosting: DigitalOcean and AWS with network segmentation, WAF, and backups.
- Payments: integrated PSPs and risk tools for fraud screening.
- KYC Providers: identity verification, PEP/sanctions screening.
- CRM & Marketing: lifecycle automation, segmentation, anti-bonus-abuse rules.
- BI & Reporting: data warehouse and dashboards for KPIs and compliance reporting.
- Ticketing: incident, change, and service requests.
- Version Control & CI/CD: controlled releases with audit trails.
- Logging & SIEM: centralised logs, alerting and retention.

8. Reporting & Communication

- Regulatory: periodic returns and notifications to the Curaçao authority; SARs as required.
- Internal: daily operations dashboard; weekly risk/compliance report; monthly management pack.
- Incident Comms: predefined templates for users, partners, and regulators.
- Board/CEO: monthly KPI review, quarterly strategy and risk review.

9. Security & Compliance

- Access Management: least privilege, MFA, quarterly recertification.
- Data Protection: encryption in transit/at rest; secure key management; retention schedule.
- Vulnerability Management: monthly scans; annual penetration testing; patch management SLAs.
- Secure Development: code reviews, secrets management, dependency checks.
- Monitoring: uptime, fraud, RG markers, and security alerts with on-call rotation.
- BC/DR: backups tested quarterly; documented recovery runbooks.

10. Appendices

A. RACI Matrix (Extended)

See Section 3 for the primary RACI. This appendix can be expanded per project or jurisdiction.

B. Risk Register Template

ID	Risk Description	Category	Likelihood	Impact	Owner	Mitigations	Status	Review Date
R-01	Payment gateway outage	Operational	Medium	High	Risk Team	Multiple PSPs; failover; monitoring	Open	YYYY-MM-DD
R-02	KYC provider downtime	Operational	Medium	Medium	Compliance	Secondary provider; manual fallback	Open	YYYY-MM-DD

C. Incident Report Template

Field	Details
Incident ID	INC-YYYY-###
Date/Time (UTC)	
Severity (SEV1–SEV3)	
Summary	
Impact (Players/Revenue/Systems)	
Root Cause	
Actions Taken	
Corrective/Preventive Actions	
Owner	

D. Change Request (CR) Form

Field	Details
CR ID	CR-YYYY-###
Title	
Description & Business Justification	
Risk & Regulatory Impact	
Test Plan & Rollback	
Approvals (Product/Compliance/CEO)	
Deployment Window	
Post-Release Checks	

E. Onboarding Checklist

- Employment agreement executed; NDA signed.
- Role description and RACI reviewed.
- Security training completed (MFA, password policy).
- Access granted per least-privilege; logged in access register.
- AML/KYC & RG training completed (within first week).
- Tools provisioned (ticketing, BI, CRM).

F. KYC Checklist (Player Due Diligence)

- Age verification and jurisdiction eligibility.
- Government ID and selfie/biometric match.
- PEP/sanctions screening; adverse media if high-risk.
- Source of funds evidence for enhanced due diligence.
- Proof of address where applicable.
- Ongoing monitoring triggers and periodic refresh.

G. Complaints Log Template

Ticket #	Date	Player ID	Summary	Status	SLA Due	Owner	Resolution
----------	------	-----------	---------	--------	---------	-------	------------

H. Training Log Template

Employee	Role	Training	Date	Result/Score	Next Refresh
----------	------	----------	------	--------------	--------------

End of Document