

INFORMATION SECURITY POLICY

Revision 2026.1

Trinity Gaming N.V.

(eboo.bet)

Table of Contents

1. Introduction	2
2. Goals	2
3. Scope	2
4. Information security principles	2
5. Responsible persons (Governance and responsibilities)	3
6. Compliance and policy awareness	3
7. Data classification and handling rules	3
8. Access control and authentication	4
9. Technical and organizational controls (baseline)	4
10. Third parties and vendors	5
11. Incident management	5
12. Business continuity and recovery	6
13. Risk management	6
14. Enforcement	6
15. Policy review and updates	6

1. Introduction

This Information Security Policy pertains to the activities carried out by:

TRINITY GAMING N.V., a limited liability company registered in Curaçao with the company number 163473, with registered address Chuchubiweg 17, Curaçao ("Company", "we", "us"),

and describes how the Company protects information and IT assets used to operate **eboo.bet** as a **B2B software aggregator**.

It sets minimum security requirements for all individuals and entities who access Company systems or data.

2. Goals

We aim to:

- protect Company and client/partner information from unauthorized access, leakage, loss, or misuse;
- reduce risks related to cyberattacks, fraud, human error, and system outages;
- maintain compliance with applicable laws and regulatory expectations (including **GDPR** and **AML-related requirements**, where relevant);
- ensure predictable, controlled handling of information security incidents.

3. Scope

This policy applies to:

- Company staff, contractors, consultants, and any authorized third parties working with Company systems;
- all IT assets supporting eboo.bet (infrastructure, applications, databases, APIs, admin panels, logs, backups);
- all data processed in the context of the Company's activities, including:
 - client and partner data (B2B accounts, contacts, contracts, billing details);
 - transactional and payment-related information (as applicable to the service);
 - operational, financial, legal, and internal corporate information;
 - any personal data processed by the Company (if/where applicable).

4. Information security principles

- **Confidentiality:** access only for authorized users with a legitimate business need.

- **Integrity:** data remains accurate and protected from unauthorized modification or deletion.
- **Availability:** systems remain reliable; recovery mechanisms exist and are maintained.
- **Compliance & accountability:** responsibilities are assigned, and controls are documented and reviewed.

5. Responsible persons (Governance and responsibilities)

- **Management:** approves this policy and ensures adequate resources for implementation.
- **Security/IT function (responsible person/team):** implements and maintains controls (access, monitoring, vulnerability handling, incident coordination).
- **Legal/Compliance / Data protection / AML functions (if applicable):** support secure handling, retention, and lawful processing of regulated datasets.
- **HR / People function (if applicable):** supports onboarding and periodic awareness activities related to security practices.
- **All users:** follow rules, protect credentials/devices, and report incidents immediately.

6. Compliance and policy awareness

- All personnel and authorized third parties must comply with this policy and related procedures.
- Security awareness is provided **on onboarding** and **periodically** thereafter (e.g., phishing/social engineering, secure handling of data, incident reporting, acceptable use).
- Users must promptly follow Company instructions during security events (e.g., password resets, device checks, temporary access restrictions).

7. Data classification and handling rules

Information is handled based on sensitivity (examples): **Public / Internal / Confidential / Restricted**.

Minimum handling requirements:

- store **Confidential/Restricted** data only in approved Company systems;
- do not export sensitive data to personal accounts, unmanaged devices, or unapproved tools;
- share sensitive data only via approved channels and only with authorized recipients;
- apply retention and deletion rules aligned with legal, regulatory, and business requirements.

8. Access control and authentication

We use a controlled access model:

- **least privilege** (minimum required permissions);
- **role-based access** and **periodic access reviews** (risk-based frequency);
- **MFA** for administrative and sensitive access where feasible/available;
- access is removed promptly when a person changes role or leaves.

Access provisioning

- Access is granted through a documented approval process (e.g., ticket/email request) and provisioned by authorized administrators.
- Privileged/admin access is limited to designated personnel and used only when necessary.

Safe password and authentication principles (baseline)

- use unique passwords (recommended **12+ characters**), avoid predictable patterns;
- never share passwords or reuse across systems;
- use an approved password manager where feasible;
- change credentials immediately if compromise is suspected or confirmed;
- where available, enable and use MFA (mandatory for admin/sensitive access).

9. Technical and organizational controls (baseline)

Network & protection

- perimeter protections (e.g., firewalls, filtering) and risk-based segmentation where applicable;
- restricted admin access (limited IPs/roles where feasible).

Secure communications

- encryption in transit (e.g., TLS/SSL) for the software and sensitive connections.

Encryption & secrets

- encryption at rest where appropriate for sensitive datasets;
- secure storage of secrets/keys; access restricted and managed (rotation/updates where feasible).

Endpoints

- devices accessing Company systems must be protected (updates, malware protection where appropriate, lock screen);
- risky or non-compliant devices may be restricted or blocked.

Vulnerability & patching

- vulnerabilities are tracked and addressed based on severity and impact;
- critical patches are prioritized.

Logging & monitoring

- security-relevant events are logged (authentication, admin actions, critical operations) where feasible;
- logs are protected from tampering and retained as required for operations/compliance.

Backups

- backups exist for critical systems/data;
- restoration is tested periodically or after major changes.

10. Third parties and vendors

Where vendors support eboo.bet (hosting, analytics, payment services, communications tools, etc.), the Company:

- evaluates risk before onboarding (proportionate to criticality);
- requires confidentiality and appropriate security standards contractually;
- limits vendor access to the minimum needed (least privilege);
- reviews key vendors periodically and upon significant changes/incidents.

11. Incident management

Any suspected security issue must be reported immediately.

High-level response approach

- **triage:** assess severity, potential impact, and scope;
- **containment:** limit damage and isolate affected assets where appropriate;
- **investigation:** identify root cause and affected data/systems (preserve evidence where feasible);
- **recovery:** restore services safely and apply corrective actions;

- **documentation:** record actions taken, findings, and improvements (“lessons learned”).

Communication and notifications

- internal communication is coordinated to ensure consistent actions and messaging;
- clients/partners are informed where contractually required or appropriate;
- if personal data or regulated data is impacted, the Company assesses notification obligations and proceeds where legally required.

12. Business continuity and recovery

- continuity and recovery measures are maintained to reduce downtime and operational impact;
- critical services/data have defined recovery approaches (risk-based);
- backups, restoration procedures, and continuity steps are tested periodically or after material changes.

13. Risk management

Security risks are reviewed regularly and upon major changes (new vendors, new features, infrastructure changes, incidents). Controls are updated to reflect:

- changing threats and vulnerabilities,
- business growth and operational changes,
- regulatory updates and contractual requirements.

14. Enforcement

Violations may result in access removal, disciplinary measures, contract termination, and/or legal action, depending on severity and applicable law/contract terms.

15. Policy review and updates

This policy is reviewed:

- at least annually; and
- after significant security, business, or regulatory changes (including material incidents).

Employees and relevant stakeholders may provide feedback for improvements; approved updates are communicated accordingly.