

INFORMATION SECURITY POLICY

This Information Security Policy (the “Policy”) sets out the framework and principles adopted by Green Point Technology N.V. (the “Company”) to ensure the confidentiality, integrity, and availability of information assets and systems related to its licensed iGaming operations under Curaçao law.

1. Purpose and Scope

The purpose of this Policy is to establish a structured approach to managing information security risks within the Company. This Policy applies to all employees, contractors, system administrators, consultants, and third-party service providers who have access to or handle Company data.

2. Information Security Objectives

- Protect all Company information systems from unauthorized access, disclosure, alteration, or destruction.
- Ensure the continuity of operations and data integrity across all platforms and services.
- Comply with applicable regulations, including Curaçao eGaming technical standards and the EU General Data Protection Regulation (GDPR).

3. Roles and Responsibilities

Chief Technology Officer (CTO): Responsible for enforcing this Policy, managing IT infrastructure, and supervising data protection measures.

Compliance Officer: Ensures that all security controls comply with regulatory and licensing requirements.

All Employees: Must adhere to this Policy and report any suspected security incidents to management immediately.

4. Access Control Policy

- Access to Company systems shall be granted based on the principle of least privilege.
- Multi-factor authentication (MFA) is required for all administrative access.
- Passwords must meet defined complexity standards and be changed at least every 90 days.
- Access rights shall be reviewed quarterly and revoked upon termination of employment.

5. Data Protection and Privacy

- All customer and financial data are encrypted both at rest and in transit.
- Backups are performed daily and securely stored in geographically redundant locations.
- Data retention periods are defined in accordance with legal and operational requirements.
- All processing of personal data follows GDPR principles of lawfulness, fairness, and transparency.

6. Network and System Security

- Firewalls, antivirus, and intrusion detection systems (IDS) are implemented across the Company's infrastructure.
- Systems are monitored for suspicious activity 24/7.
- Security patches and software updates are applied promptly.
- Remote connections are protected through VPN and encryption protocols.

7. Incident Response Plan

- All incidents must be reported immediately to the CTO and documented in the Incident Register.
- The CTO is responsible for assessing the severity and initiating appropriate mitigation actions.
- Post-incident reviews are conducted to identify root causes and prevent recurrence.

8. Third-Party Providers and Integrations

- All third-party providers, including payment service providers and platform vendors, must undergo due diligence and security assessment.
- Data exchange with third parties must occur through secure, encrypted APIs.
- Contracts with third parties must include confidentiality and data protection clauses.

9. Business Continuity and Disaster Recovery

- The Company maintains a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to minimize downtime.
- Critical systems are backed up daily with a defined recovery time objective (RTO) of 4 hours.
- Regular testing of recovery procedures is performed annually.

10. Training and Awareness

- All employees receive mandatory security awareness training annually.
- Phishing simulations and data protection workshops are conducted periodically.

11. Review and Updates

This Policy is reviewed at least once per year or upon significant organizational or technological changes. The CTO, in coordination with the Compliance Officer, is responsible for maintaining and updating this Policy.

Signature:  _____

Maria Eleni Gkioka

Chief Technology Officer

Green Point Technology N.V.

Date: 24/10/2025