



Information Security Policy

Version Control

VERSION	UPDATE	AUTHOR	DATE
1.0	Document Creation	Compliance Officer	26 May 2025

Contents

Version Control.....	2
1. Introduction	4
2. Purpose	4
3. Scope.....	4
4. Roles and Responsibilities	5
5. Internal Information Security Guidelines	5
5.1. Acceptable Use.....	5
5.2. Password Management	5
5.3. Access Control	5
5.4. Data Classification and Handling.....	6
5.5. Device and Endpoint Security	6
5.6. Security Awareness and Training	6
6. External Threat Protection	6
6.1. Phishing and Social Engineering	6
6.2. Scams and Fraud Detection.....	6
6.3. Protection Against Hacking	7
6.4. Secure Software Development	7
6.5. Protection Against new Programs	7
7. Incident Response and Reporting	7
8. Regulatory and Legal Compliance	7
9. Policy Review	7

1. Introduction

This is the Information Security Policy of Moonrail Limited B.V. (the “Company” or “Moonrail”). This Policy has been designed to help improve the information security on the Company’s information assets. It further outlines the Company’s commitment to protect these assets at all costs from unauthorized access, use, modification, disruption and modification of any sorts.

2. Purpose

The purpose of this Information Security Policy is to establish a framework that safeguards the confidentiality, integrity and availability of Moonrail’s Information Technology System (“IT System”). The Company understands that secure management of information assets is critical to sustaining the trust of customers, the reliability of its business functions, and its adherence to legal and regulatory requirements. This policy, thus, aims to:

- Minimize risk exposure related to data breaches and cyber threats.
- Foster a security-conscious culture across the Company.
- Safeguard client data, internal communications, and proprietary business information.
- Comply with applicable regulatory, legal, and contractual obligations.

3. Scope

This policy applies to:

- All employees, consultants, temporary staff, contractors, third-party service providers who will interact directly or indirectly with the company’s IT System.
- All data, systems, applications and network resources owned, managed, leased or operated by Moonrail or its subsidiary that has direct or indirect access to the Company’s IT System.
- All external stakeholders interacting with Moonrail’s gambling platform(s) or digital infrastructure.

4. Roles and Responsibilities

- Management is responsible for the enforcement of this Policy and the appointment of Senior IT Officers.
- Senior IT Officers are tasked with overseeing the IT Security Team. They are responsible for setting up technical protections, supervising the IT Team and handling of any incident reports.
- The IT Security Team is responsible for ensuring that the staff members follow security policies and best practices. They shall monitor activities and provide guidance to maintain a secure environment.
- All staff members must fulfill their obligations which include attending mandatory training at least once a year, following the security policies, and reporting any suspicious activity.
- Contractors and third- party service providers must adhere to security standards as may be defined in the contracts.

5. Internal Information Security Guidelines

5.1. Acceptable Use

All computing resources must be used only for company-approved activities. Email and internet access are strictly intended for business use. Limited personal use of Company 's devices is allowed, if it does not interfere with work or compromise the security of the IT systems.

5.2. Password Management

The Company requires that strong, unique passwords must be used for all Company systems. Multi-Factor Authentication (MFA) is required for accessing parts of the IT Systems containing ultra-sensitive information such as customer data and transactions.

5.3. Access Control

The Company applies the principle of least privilege with respect to granting access to the IT System of the Company. Employee access is reviewed regularly and removed when roles change or upon termination of employment.

5.4. Data Classification and Handling

Data must be classified as:

- **Public:** Openly shareable.
- **Internal:** For employees only.
- **Confidential:** Sensitive data needing encryption and limited access.
- **Highly sensitive:** limited to essential personnel only.

Customer -and operational data are deemed highly confidential and must be encrypted when stored or transmitted. Access to such data should be strictly controlled.

5.5. Device and Endpoint Security

All devices must have company-managed antivirus and anti-malware tools installed on them. Devices should be kept up to date and must be locked whenever left unattended.

5.6. Security Awareness and Training

All employees must complete a mandatory security training upon employment with the Company and annually thereafter. Phishing simulations and awareness campaigns are regularly conducted.

6. External Threat Protection

6.1. Phishing and Social Engineering

All email and communication platforms and tools are monitored for suspicious activity. Customers are educated to on spot phishing attempts through platform messages and support channels.

6.2. Scams and Fraud Detection

The Company uses third party anti-fraud tool (SEON) to monitor gaming activity for unusual patterns. Financial transactions are also screened for irregularities.

6.3. Protection Against Hacking

The web platforms and mobile applications undergo regular testing for vulnerabilities. Security measures such as firewalls, intrusion detection/prevention systems (IDS/IPS), and DDoS mitigation tools are employed to safeguard against potential threats.

6.4. Secure Software Development

Code is reviewed, tested and scanned for vulnerabilities before it goes live. An Internal Bounty program is encouraged to assure any possible Gap in Coding is discovered internally and fixed accordingly.

All third-party service providers vetted to ensure compliance with security standards. for security compliance.

6.5. Protection Against new Programs

Downloads are Blocked and will require administrator approval. The installation of new programs is also restricted and require administrator approval.

7. Incident Response and Reporting

Any security incident must be reported immediately to a Senior IT Officer.

The incident response team will then assess, contain and resolve the breach following established procedures. If customers are affected, the breach will be disclosed transparently in line with regulatory requirements.

8. Regulatory and Legal Compliance

The company complies with the Curaçao Gaming Authority's requirements and applicable data protection laws. Regular (internal) audits are conducted to ensure compliance with internal and external security standards.

9. Policy Review

This policy is reviewed annually, or upon significant changes to the operations, information technology threats and/or regulatory requirements.