

Information Security Policy

Coinbar N.V.

Groot Kwartierweg 10

Livestrong Building

Curacao

Curacao License Number: OGL/2024/920/0382

Table of Contents:

1. Introduction
2. Scope
3. Objectives
4. IT Resources and Infrastructure
5. Data Uploading, Storage, and Protection
6. Application Security
7. Security Incident Management
8. Employee Responsibilities
9. Vendor and Third-Party Security
10. Policy Enforcement and Review
11. Contact Information

1. Introduction

This Information Security Policy establishes the framework for protecting the confidentiality, integrity, and availability of all data and systems within Coinbar N.V., an online gaming operator licensed in Curacao. It aims to safeguard company assets, customer data, and maintain regulatory compliance.

2. Scope

This policy applies to all employees, contractors, vendors, and third-party service providers with access to Coinbar's IT resources, data, and applications.

3. Objectives

- Protect sensitive and proprietary data from unauthorized access, alteration, or disclosure.
 - Ensure the integrity and availability of gaming systems and data.
 - Minimize cybersecurity risks through proactive measures.
 - Comply with local (Curacao) and international data protection regulations.
-

4. IT Resources and Infrastructure

4.1 Hardware and Network Resources

- All servers, workstations, network devices, and communication infrastructure must be configured securely, regularly maintained, and monitored for suspicious activity.
- Hardware shall undergo routine inspections, firmware, and software updates.

4.2 Software and Applications

- Only authorized software and applications approved by the IT security team may be installed and used.
- Software updates and patches must be applied promptly to fix vulnerabilities.

4.3 Access Management

- Access to IT resources is granted based on the principle of least privilege.
- Multi-factor authentication (MFA) shall be implemented for all critical systems.

- User accounts must be unique, and sharing of credentials is prohibited.
-

5. Data Uploading, Storage, and Protection

5.1 Data Uploading

- Data transfers must utilize secure protocols such as SFTP and HTTPS.
- All data uploads must be logged, verified, and monitored for integrity.

5.2 Data Storage

- Data shall be stored in encrypted databases or storage systems using industry-standard encryption algorithms (e.g., AES-256).
- Access to stored data is limited to authorized personnel only, with clear audit trails maintained.

5.3 Data Backup and Recovery

- Regular backups of all critical data shall be performed daily, with backups stored securely off-site or in geographically dispersed locations.
- Backup procedures shall include verification steps to ensure data integrity and completeness.
- A disaster recovery plan shall be maintained and tested periodically.

5.4 Data Protection and Privacy

- Data must be protected from unauthorized access, modification, or destruction.
 - Personal and customer data must comply with relevant data protection laws, including GDPR and Curacao privacy laws.
 - Data retention policies shall define how long data is stored before secure deletion.
-

6. Application Security

- All applications utilized within the organization must undergo security assessments prior to deployment.
- Applications shall be configured following security best practices, including secure coding standards, input validation, and session management.
- Regular vulnerability scans and penetration tests shall be conducted to identify and remediate security flaws.

7. Security Incident Management

- All security incidents must be promptly reported to the IT security team.
- An incident response plan is in place to address, contain, and remediate security breaches.
- Post-incident reviews shall analyze root causes and implement corrective actions.

8. Employee Responsibilities

- Employees must adhere to all security policies and procedures.
- Security awareness training shall be conducted regularly.
- Confidentiality agreements must be signed by all personnel handling sensitive data.

9. Vendor and Third-Party Security

- Vendors and third-party providers with access to company systems must comply with this security policy.
- Security assessments of vendors shall be conducted prior to engaging with them.

10. Policy Enforcement and Review

- Compliance with this policy is mandatory; violations may result in disciplinary action.
- The policy shall be reviewed annually or following significant changes to systems or regulations.

11. Contact Information

For questions or security concerns, contact:

IT Security Team: manager@coinbar.com

Coinbar N.V. is committed to maintaining the highest standards of information security to ensure the trust of our customers, partners, and regulatory bodies.
