

Information Security Policy

Company Information

Company Name: Leopard B.V.

Brand(s): CaratCasino

Website: www.caratcasino.com

License Number: OGL/2024/793/0757

Regulator: Curaçao Gaming Authority (CGA)

Effective Date: 11.11.2025

1. Purpose

This policy establishes the framework for maintaining the confidentiality, integrity, and availability of all information assets managed by Leopard B.V. It ensures compliance with CGA and aligns with ISO/IEC 27001 standards.

2. Scope

Applies to all employees, contractors, and third parties; all IT systems, networks, and databases; and all customer and operational data.

3. Information Security Objectives

- Protect company and customer data
- Ensure operational resilience
- Maintain compliance with CGA and GDPR
- Assign clear security responsibilities
- Continually improve through audits and monitoring

4. Roles and Responsibilities

Board: oversight and resources.

CISO/Security Officer: lead information security.

IT Department: implement controls.

Employees: comply and report incidents.

5. Data Classification

Data is classified as: Public, Internal, Confidential, or Highly Confidential — with corresponding access restrictions.

6. Access Control

Use of unique user IDs, MFA, least-privilege access, periodic reviews, and immediate deactivation upon termination.

7. Network and System Security

Servers hosted in Tier-IV datacenters in Curaçao. Firewalls, IDS/IPS, encryption (TLS 1.2+), and regular penetration tests are mandatory.

8. Data Protection and Privacy

Compliance with GDPR and CGA Data Protection standards. Data encrypted at rest and in transit, retained for up to 5 years after account closure.

9. Incident Management

All incidents reported to the Security Officer and MLRO. Immediate containment, investigation, and notification to CGA within 72 hours if required.

10. Business Continuity and Disaster Recovery

Maintain BCP and DRP to ensure service continuity. Backups encrypted and tested quarterly.

11. Vendor and Third-Party Management

All vendors undergo due diligence, must comply with GDPR and CGA, and are reviewed annually.

12. Employee Awareness and Training

Mandatory onboarding and annual training covering passwords, phishing, data handling, and incident reporting.

13. Monitoring, Logging, and Auditing

Security logs retained for 12 months, reviewed regularly, and audited annually by CGA-approved assessors.

14. Policy Violations

Violations may result in disciplinary actions, access suspension, or regulatory reporting.

15. Review and Updates

Reviewed annually or upon regulatory/operational changes or post-incident updates.