

Information Security Policy

Effective Date: June 2025

Last Reviewed: June 2025

INTRODUCTION

This Information Security Policy (ISP) provides a comprehensive framework to ensure data and system security across Goldeneggs.casino's operations.

The website <https://goldeneggs.casino/> ("Casino", "Website", "Company", "We", "Us", "Our") is owned and operated Peak Progress Partners N.V., a company registered in accordance with Curacao Law, registration No.167287, Address: Trias Building, Hanchi Snoa 19, Willemstad, Curaçao.

This ISP has been developed in accordance with The National Ordinance on the Protection of Personal Data (Landsverordening Bescherming Persoonsgegevens), Curacao Gaming Authority (CGA) requirements, Landsverordening op de Kansspelen (LOK), AML/CFT laws of Curacao, General Data Protection Regulation (EU) 2016/679 ("GDPR") and international standards such as ISO/IEC 27001.

SCOPE AND INFORMATION COLLECTED

This ISP applies to all platforms, IT infrastructure, employees, third-party vendors, and digital environments related to Goldeneggs.casino's services.

The provisions regarding the collection of personal information (e.g. full name, residential address, date of birth, place of birth, e-mail address, telephone number or other relevant information) are described in a separate Privacy Policy publicly available on our Website.

We hold all information on secure servers based in Netherlands and elsewhere from time to time.

ACCESS MANAGEMENT

Goldeneggs.casino enforces a robust access control framework based on the Principle of Least Privilege (PoLP). Access to systems and data is granted based on Role-Based Access Control (RBAC). This sub-approach ensures that users have access only to the resources necessary to perform their job functions. All administrative and system-level access requires Multi-Factor Authentication (MFA).

Access logs are retained and reviewed for anomalies. Immediate revocation is applied upon termination of employment or change of role (typically, departing personnel accounts are deactivated within 24 hours).

DATA PROTECTION

Goldeneggs.casino understands the importance of security and the techniques needed to secure information and data.

To safeguard sensitive and personal information in accordance with Curaçao legislation, GDPR, other global best practices, Goldeneggs.casino implements advanced cryptographic mechanisms:

- Data at rest, including databases, backups, and file storage, is encrypted using AES-256 or higher;
- Data in transit is secured using TLS 1.3 with Perfect Forward Secrecy (PFS);
- Encryption keys are stored in a hardware-based key management system (HSM) and rotated bi-annually or upon compromise.

In addition, sensitive data is anonymized when possible to reduce exposure.

MONITORING AND LOGGING

All system, network, application, and user/customer access logs are captured and stored in an immutable and tamper-evident log management solution. Logs are retained for a minimum of five (5) years in compliance with AML/CFT recordkeeping requirements.

A Security Information and Event Management (SIEM) system is used to aggregate, correlate, and analyze events in real time, facilitating detection of threats such as account compromise, privilege escalation, and suspicious network behavior.

INCIDENT RESPONSE

Goldeneggs.casino maintains an Incident Response Plan (IRP). The IRP defines:

- Roles and responsibilities of the incident response team;
- Classification and escalation procedures;
- Communication protocols (internal and external);
- Notification procedures to CGA, FIU, and affected data subjects (incidents are reported to CGA and FIU within 24 hours if required).

All incidents are logged and post-incident reviews are conducted to update IPS and reduce recurrence.

All incidents are triaged based on severity, and critical findings are remediated within 72 hours.

Also incident documentation is maintained and reviewed during annual audits.

APPLICATION AND INFRASTRUCTURE SECURITY

Goldeneggs.casino implements Secure Software Development Lifecycle (SSDLC) practices:

- All source code undergoes peer review and is scanned using Static Application Security Testing (SAST) tools;
- Dynamic Application Security Testing (DAST) and penetration tests are performed on deployed applications;
- Secure coding principles (OWASP Top 10) are enforced.

Infrastructure is hosted in a secure, audited environment with firewalls, IDS/IPS, DDoS mitigation, and network segmentation between development, staging, and production systems.

BACKUP AND RECOVERY

Daily encrypted backups are automatically created and stored in redundant, geographically separated locations. Backups are subject to regular restore tests to verify integrity.

The following disaster recovery objectives apply:

- Recovery Time Objective (RTO): 4 hours;
- Recovery Point Objective (RPO): 12 hours.

THIRD-PARTY PRACTICES

Goldeneggs.casino used third-party electronic payment systems to process such financial transactions.

Third-party vendors and service providers are subject to a risk-based due diligence process.

TRAINING

All staff of Goldeneggs.casino receive onboarding and annual refresher training on information security awareness, including phishing, password management, and data handling.

Specialized training modules are provided to developers (secure coding), system administrators (infrastructure hardening), and customer support (data privacy obligations).

Participation in the training is mandatory and tracked.

All training modules are reviewed and updated annually to reflect emerging threats and regulatory changes.

AUDITING

This ISP is subject to annual internal review by the Information Security Officer or by the Compliance team.

Independent third party audits may be conducted as needed and requested by CGA.

Any non-conformities are documented and resolved with a Corrective Action Plan (CAP).

DATA RETENTION AND DESTRUCTION

Retention of user/customer records, system logs, and financial data is mandated for a minimum of five (5) years post business relationship, as per AML/CFT requirements.

All paper-based sensitive materials are shredded.

CONTACT AND SUPPORT

For any questions related to this IPS, please contact:

Email: support@goldeneggs.casino, compliance@goldeneggs.casino

APPROVED BY:

Name:

Position:

Date: