



# Information Security Policy

## (Curaçao LOK Compliant)

*Geeker Technology N.V*

**Effective Date: 29/06/2025**

**Approved By: Felix Chelu**

**Last Review Date: 01/09/2025**

**Next Review Date: 01/02/2026**

---

### 1. Purpose & Scope

The purpose of this Information Security Policy (ISP) is to establish the framework for protecting Geeker NV's information assets, ensuring the confidentiality, integrity, and availability of all systems and data, and maintaining compliance with the Curaçao LOK regulations.

This policy applies to all Geeker NV employees, contractors, systems, networks, applications, and data, including third-party services utilized for online gaming operations.

---

### 2. Roles & Responsibilities

- **IT & Security Team:** Enforces security measures, monitors systems, responds to incidents.
  - **Employees:** Adhere to security practices, report incidents.
  - **Incident Response Team:** Responds to security incidents, coordinates reporting to management and CGA.
- 

### 3. Risk Assessment & Management

- Conduct regular risk assessments for all systems and networks.
- Identify potential threats including cyber-attacks, insider threats, fraud, and DDoS.

- Implement risk mitigation controls and review them annually.
- 

#### **4. Access Control**

- Enforce strong authentication (password policy, MFA).
  - Apply least privilege and role-based access controls.
  - Review access rights periodically.
  - Ensure proper onboarding and offboarding procedures
- 

#### **5. Data Protection**

- Classify data (personal, financial, sensitive).
  - Encrypt data in transit and at rest.
  - Securely store backups and manage data retention/deletion.
  - Ensure compliance with applicable privacy regulations.
- 

#### **6. Network & System Security**

- Maintain secure network design with segmentation and firewalls.
  - Configure servers and applications securely.
  - Regularly patch systems and manage vulnerabilities.
  - Monitor and log system activities; retain logs securely.
- 

#### **7. Third-Party & Supplier Security**

- Conduct due diligence on third-party providers.
- Include security requirements in contracts.

- Monitor and audit critical third-party systems.
- 

## **8. Incident Response & Breach Management**

- Define and categorize security incidents.
  - Respond promptly with containment, eradication, and recovery plans.
  - Notify management and Curaçao Gaming Authority (CGA) for significant breaches.
  - Conduct post-incident reviews and implement lessons learned.
- 

## **9. Business Continuity & Disaster Recovery**

- Implement backup strategies for all critical systems.
  - Maintain recovery procedures for system failures, disasters, and ransomware attacks.
  - Regularly test business continuity and disaster recovery plans.
- 

## **10. Change & Configuration Management**

- Document and approve changes to systems.
  - Test changes prior to deployment.
  - Maintain rollback procedures.
- 

## **11. Physical Security**

- Control physical access to offices, server rooms, and data centers.
  - Implement environmental protections (power, cooling, disaster prevention).
- 

## **12. Monitoring, Auditing & Reporting**

- Conduct regular internal and external security audits.
  - Perform penetration testing and vulnerability scanning.
  - Report audit findings to management and CGA as required.
- 

### **13. Training & Awareness**

- Provide security awareness training to all employees.
  - Deliver specialized training for technical and key personnel.
- 

### **14. Compliance & Regulatory Requirements**

- Ensure compliance with Curaçao LOK regulations, including safe systems, incident reporting, and local substance requirements.
  - Comply with applicable data protection regulations.
  - Align AML/KYC processes with information security requirements.
- 

### **15. Review & Updates**

- Review the ISP at least annually or upon significant changes.
- Update policy based on audit findings, threat landscape, or regulatory changes.