



INFORMATION SECURITY POLICY

Trickless N.V. (the “Company”)

Effective Date: [30/05/2025]

Reviewed Annually | Approved by: [Compliance Lead Name]

Information Security Policy

Trickless N.V. | License GLH-OCCHKTW0708062022

Effective Date: [Insert Date]

Reviewed Annually | Approved by: [Compliance Lead Name]

1. Purpose & Scope

This policy defines the principles and controls used to protect the integrity, confidentiality, and availability of all data handled by Trickless N.V., in compliance with the Curaçao Gaming Authority (CGA), GDPR, and related gaming legislation.

2. Governance & Oversight

- Appoint a Responsible Gaming Officer and Information Security Manager.
 - Register with goAML for AML compliance and suspicious transaction reporting.
 - Ensure all company stakeholders meet CGA integrity requirements.
 - Complete annual reviews and report policy effectiveness to senior leadership.
-

3. Data Protection & Privacy

- Encrypt all sensitive data using AES-256 standards.
 - Store player and system logs securely with access restrictions.
 - Retain AML-relevant data for a minimum of 5 years per CGA regulations.
 - Comply with GDPR rights including data access, portability, and erasure.
-

4. Access Control & Authentication

- Implement role-based access and enforce least-privilege principles.
 - Apply multi-factor authentication to all administrative access points.
 - Conduct quarterly access reviews and terminate unused credentials promptly.
-

5. Incident Response & Breach Protocol

- Maintain and test a formal Incident Response Plan (IRP).
 - Notify the CGA within 72 hours of any confirmed data breach.
 - Document root cause analysis and maintain breach records for audit.
-

6. Responsible Gaming & Player Safeguards

- Monitor account patterns for indicators of problem gambling.
 - Technically enforce:
 - Deposit and loss limits
 - Session time caps
 - Self-exclusion requests
 - Ensure players have access to dispute resolution channels and RG tools.
-

7. Third-Party Risk Management

- Vet all vendors for cybersecurity posture and regulatory alignment.
 - Require data protection agreements with game providers and processors.
 - Validate Curaçao-based suppliers hold appropriate CGA certifications.
-

8. Policy Review & Continuous Improvement

- Conduct internal and external audits annually.
- Update controls based on evolving threat landscapes or regulatory shifts.
- Track completion of action items from compliance assessments.

Appendix: Staff Security Training Checklist

Cybersecurity Awareness

- ☐ Identify phishing, spoofing, and social engineering risks
- ☐ Practice strong password hygiene and enable MFA
- ☐ Lock devices when unattended
- ☐ Avoid public networks when accessing work platforms
- ☐ Report any suspected breach or irregularity

Platform Access & System Controls

- ☐ Use VPN when connecting remotely
- ☐ Understand role-based permissions and system limits
- ☐ Never share credentials or authentication tokens
- ☐ Follow protocols for file downloads and updates

Regulatory Compliance

- ☐ Understand Curaçao Gaming Authority obligations
- ☐ Apply GDPR principles in everyday workflows
- ☐ Monitor for AML red flags and escalate unusual activity
- ☐ Follow KYC documentation procedures for new and withdrawing players

Privacy & Data Handling

- ☐ Safeguard physical and digital player records
- ☐ Respect data retention periods and secure deletion protocols
- ☐ Use secure messaging platforms for internal communication

Incident Response Readiness

- [] Know your role in breach scenarios
- [] Complete simulation exercises at least once per year
- [] Record breach indicators and assist in containment measures

Responsible Gaming Principles

- [] Detect behavioral signs of addiction or loss-chasing
- [] Uphold RG tools such as deposit limits and play suspensions
- [] Avoid marketing tactics targeting vulnerable demographics