

trickles2

INFORMATION SECURITY POLICY

Trickless N.V. (the "Company")

Effective Date: [30/12/2025] Version:2.0

Information Security Policy

Trickless N.V. (the "Company")

License: GLH-OCCHKTW0708062022

Effective Date:30/12/2025

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.

All controls described below are currently in place and subject to ongoing review and improvement.

2. Governance & Oversight

- Responsible Gaming Officer and Information Security Manager appointed.
 - Registered with goAML for AML compliance and suspicious transaction reporting.
 - All stakeholders meet CGA integrity requirements.
 - Annual reviews and risk assessments conducted; effectiveness reported to senior leadership.
-

3. Data Protection & Privacy

- All sensitive data encrypted using AES-256 or stronger (at rest and in transit).
 - Player and system logs stored securely with access restrictions and audit trails.
 - AML-relevant data retained for minimum 5 years per CGA regulations.
 - GDPR rights (access, portability, erasure) fully supported.
 - Privacy notices and data processing agreements reviewed and updated regularly.
-

4. Access Control & Authentication

- Role-based access and least-privilege principles enforced.
- Multi-factor authentication (MFA) applied to all administrative access points.
- Quarterly access reviews; unused credentials terminated promptly.
- All access and changes to critical systems logged and reviewed.

5. System Security

- Regular patching and updates for all software, systems, and network devices.
 - Firewalls, anti-malware, and intrusion detection/prevention systems deployed.
 - Regular vulnerability assessments and penetration testing performed.
 - Physical access to servers, offices, and data centers secured; visitor logs maintained.
-

6. Incident Response & Breach Protocol

- Formal Incident Response Plan (IRP) maintained and tested annually.
 - Confirmed data breaches reported to CGA within 72 hours via license management portal.
 - Root cause analysis documented; breach records maintained for audit.
 - Regular incident response drills; staff trained on breach roles.
-

7. Responsible Gaming & Player Safeguards

- Account patterns monitored for problem gambling and suspicious activity.
 - Deposit/loss limits, session time caps, and self-exclusion requests enforced.
 - Players have access to dispute resolution channels (including certified ADR providers) and RG tools.
 - Player data and privacy protected in all RG-related processes.
-

8. Third-Party Risk Management

- All vendors vetted for cybersecurity posture and regulatory alignment.
 - Data protection agreements in place with all game providers and processors.
 - Curaçao-based suppliers validated for CGA certifications.
 - Third-party compliance monitored; contracts reviewed regularly.
-

9. Policy Review & Continuous Improvement

- Internal and external audits conducted annually.
- Controls updated based on evolving threats, regulatory shifts, or audit findings.
- Action items from compliance assessments tracked to completion.
- Policy reviewed and updated at least annually or after significant changes.



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

