

Information Security Policy of WP Consulting N.V.

For Weplay Network

Policy Version: Last updated on May 15, 2025

1. Introduction

1.1. Company Overview:

WP Consulting N.V. operates [WePlay Network](#), with its office located at Zuikertuintjeweg Z/N, Willemstad, Curacao, under registration number 156492.

1.2. Information Security Policy Objectives:

The primary objective of the Information Security Policy for Weplay Network (WP Consulting N.V.) is to safeguard the confidentiality, integrity, and availability of player data, financial transactions, and IT systems while ensuring compliance with regulatory standards and fostering trust.

2. Definitions

- **Data Breach:** Unauthorized access, disclosure, or loss of sensitive data.
- **Personally Identifiable Information (PII):** Data that identifies individuals (e.g., names, IDs, payment details).
- **Encryption:** Process of converting data into a secure format to prevent unauthorized access.
- **Multi-Factor Authentication (MFA):** Security protocol requiring multiple verification methods for access.
- **Malware:** Malicious software designed to disrupt or damage systems.

3. Policy Overview

Weplay Network, operated by WP Consulting N.V. (CGA License **OGL/2024/113/0114**), is committed to safeguarding player data, financial transactions, and IT infrastructure. This policy aligns with **CGA regulations, GDPR, and ISO 27001 standards**, ensuring confidentiality, integrity, and availability of information.

4. Mandatory Requirements

Weplay Network implements the following **core security measures**:

- **Encryption:** AES-256 encryption for data at rest and TLS 1.3 for data in transit.
- **Access Controls:** Role-based access to sensitive systems and data.
- **Incident Response:** Formal protocols for breach detection, containment, and reporting.
- **Regular Audits:** Annual penetration testing and vulnerability assessments.

5. Data Protection Measures

5.1 Data Classification

- **Tier 1 (Critical):** Payment details, government IDs.
- **Tier 2 (Confidential):** Player account data, transaction history.
- **Tier 3 (Public):** Marketing content, non-sensitive website data.

5.2 Access Controls

- **MFA:** Required for all employee and third-party access to critical systems.
- **Least Privilege Principle:** Employees granted minimum access necessary for their role.
- **Session Timeouts:** Automatic logout after 15 minutes of inactivity.

5.3 Network Security

- **Firewalls:** Next-gen firewalls to block unauthorized traffic.
- **Intrusion Detection Systems (IDS):** Real-time monitoring for suspicious activity.
- **VPNs:** Mandatory for remote access to internal networks.

5.4 Endpoint Protection

- **Antivirus Software:** Regular updates and scans on all devices.
- **Patch Management:** Automatic updates for OS and critical software.

6. Incident Response & Management

6.1 Breach Detection

- **Monitoring:** 24/7 SIEM (Security Information and Event Management) tools.
- **Alerts:** Immediate notifications for unauthorized access or anomalies.

6.2 Containment & Investigation

- **Isolation:** Disconnect affected systems to prevent spread.
- **Forensics:** Partner with cybersecurity experts to identify root causes.

6.3 Notification

- **Regulators:** Report breaches to CGA within **72 hours**.
- **Players:** Notify impacted users if PII is compromised.

6.4 Post-Incident Review

- **Lessons Learned:** Document improvements to prevent recurrence.

7. Third-Party Risk Management

- **Vendor Audits:** Annual security assessments for partners (e.g., payment processors).
- **Contracts:** Include clauses requiring GDPR/CGA compliance and data protection.
- **API Security:** OAuth 2.0 for secure third-party integrations.

8. Staff Training & Governance

8.1 Information Security Officer (ISO)

- **Role:** Oversee policy implementation, incident response, and audits.
- **Reporting:** Quarterly updates to executive management and CGA.

8.2 Training Programs

- **Topics:** Phishing awareness, password hygiene, breach reporting.
- **Frequency:** Bi-annual training for all employees.

9. Compliance & Reporting

9.1 Audits

- **Internal:** Quarterly reviews of access logs and system configurations.
- **External:** Annual ISO 27001 audits by certified third parties.

9.2 Documentation

- **Retention:** Security logs retained for **7 years**.
- **CGA Reporting:** Submit audit results and incident reports on request.

10. Policy Accessibility

- **Languages:** Available in English and other primary target markets.
- **Distribution:**
 - Shared with employees via internal portals.
 - Publicly accessible on Weplay Network's homepage footer.
- **Contact:** Report security concerns to support@we-play.poker.

11. Policy Review and Updates

Annual Review: This policy must be reviewed annually or whenever there is a significant change in regulations or Weplay Network's business operations.

Staff Training: Regular training sessions on all employees will be conducted for employees.

WP Consulting N.V.

By: Mitja Javornik, Director

Signature:  _____