



POPIPLAY

Information Security Policy (ISP)

Version: 1.0

Company Name: PP Solutions N.V. (POPIPLAY)

License Number: OGL/2024/190/0180

Effective Date: 13.05.2026.

1. Purpose

The purpose of this Information Security Policy (“Policy”) is to establish the principles, rules, and controls adopted by PP Operations d.o.o. (“Company”) to protect information assets, customer data, gaming systems, payment systems, and operational infrastructure from unauthorized access, disclosure, alteration, destruction, or disruption.

This Policy supports compliance with applicable:

- Curaçao Gaming Authority (CGA) licensing requirements;
- Data protection and privacy regulations;
- Anti-Money Laundering (AML) obligations;
- Responsible gaming obligations;
- Internal governance and operational security standards.

2. Scope

This Policy applies to:

- All employees;
- Directors and management;
- Contractors and consultants;
- Third-party service providers;
- All information systems operated or managed by the Company.
- The Policy covers:
- Customer information;



- Financial information;
- Gaming systems;
- Payment systems;
- Internal business information;
- IT infrastructure;
- Cloud services;
- Communication systems;
- Backup systems.

3. Information Security Objectives

The Company shall maintain appropriate safeguards to ensure:

3.1 Confidentiality

Information is accessible only to authorized individuals.

3.2 Integrity

Information is accurate, complete, and protected from unauthorized modification.

3.3 Availability

Systems and information remain available to authorized users when required.

3.4 Compliance

Operations comply with legal, regulatory, and contractual obligations.

4. Roles and Responsibilities

4.1 Management

- Management is responsible for:
- Approving this Policy;
- Providing adequate resources;
- Ensuring compliance;
- Reviewing security risks regularly.

4.2 Information Security Officer

- The Information Security Officer (ISO) is responsible for:
- Monitoring security controls;



- Conducting risk assessments;
- Managing incidents;
- Coordinating audits;
- Maintaining security documentation.

Assigned Officer: Boris Ceranic / Head of Architecture & Security

4.3 Employees and Contractors

All personnel must:

- Follow this Policy;
- Protect confidential information;
- Report security incidents immediately;
- Use company systems responsibly.

5. Information Security Risk Management

The Company shall maintain a documented information security risk management process to identify, assess, mitigate, monitor, and review risks affecting systems, infrastructure, gaming operations, customer data, and third-party services.

Risk assessments shall:

- Be conducted periodically and following significant operational or infrastructure changes;
- Evaluate threats, vulnerabilities, likelihood, and business impact;
- Assign risk ownership and remediation responsibilities;
- Be reviewed by management;
- Be documented and retained for audit purposes.
- Security controls shall be implemented using a risk-based approach and prioritized according to operational and regulatory impact.

6. Asset Management

The Company shall maintain an inventory of:

- Hardware assets;
- Software assets;
- Databases;
- Cloud infrastructure;
- Gaming systems;



- Critical business applications.

Assets shall be classified according to sensitivity:

- Public;
- Internal;
- Confidential;
- Restricted.

The Company shall apply appropriate handling, storage, retention, and access requirements according to asset classification.

7. Access Control Policy

7.1 User Access Management

Access to systems shall be:

- Role-based;
- Limited to business necessity;
- Approved by management;
- Reviewed periodically.

The Company shall apply the principles of least privilege and need-to-know access.

7.2 Authentication Requirements

The following controls shall apply:

- Unique user accounts;
- Strong password policies;
- Multi-factor authentication (MFA) for administrative and critical systems;
- Automatic account lockout after three (3) failed attempts.

7.3 Privileged Access

Administrative access shall:

- Be restricted to authorized personnel only;
- Be logged and monitored;
- Be reviewed periodically.

Privileged accounts shall not be shared unless technically required and formally approved.

7.4 Remote Access and Endpoint Security



Remote access to Company systems shall:

- Require secure VPN or equivalent encrypted connections;
- Use Company-approved authentication methods;
- Be restricted to authorized personnel.

Company devices and endpoints shall:

- Use endpoint protection solutions;
- Maintain current security patches;
- Be protected against unauthorized software installation where applicable.

8. Network and Infrastructure Security

The Company shall implement:

- Firewalls;
- Intrusion detection and prevention systems;
- Network segmentation;
- Anti-malware protection;
- Endpoint protection;
- Secure VPN access;
- Encryption for data transmission.

All production systems shall:

- Receive security updates regularly;
- Be monitored continuously;
- Be protected against unauthorized access.

Cloud-hosted infrastructure shall be configured according to industry security best practices and subject to continuous monitoring and access control oversight.

The Company shall maintain logical and/or physical segregation mechanisms to prevent unauthorized access between customer/operator environments and data.

9. Data Protection and Encryption

9.1 Client Data Protection

Client information shall be protected against unauthorized access, disclosure, alteration, or misuse.



The Company shall implement appropriate controls to ensure data confidentiality, integrity, and availability.

9.2 Encryption

Sensitive information shall be encrypted:

- In transit using TLS/SSL;
- At rest using industry-standard encryption.

9.3 Data Retention

Data shall be retained according to:

- Regulatory requirements;
- AML obligations;
- Operational requirements.

Data retention and disposal processes shall ensure secure deletion or destruction where applicable.

10. Secure Software Development

The Company shall apply secure development practices including:

- Code reviews;
- Vulnerability scanning;
- Penetration testing;
- Change management procedures;
- Separation between development, testing, and production environments.

External penetration testing shall be conducted at least annually and following significant infrastructure or application changes.

The Company shall maintain secure change management procedures to ensure changes are reviewed, tested, approved, and documented before deployment to production environments.

Third-party software providers shall be subject to due diligence and security evaluation.



11. Vulnerability and Patch Management

The Company shall maintain processes for identifying, assessing, prioritizing, and remediating security vulnerabilities affecting systems and applications.

Vulnerability assessments and automated scanning shall be conducted periodically.

Security patches shall be applied according to risk severity and operational requirements.

Target remediation timelines shall generally follow:

Severity	Target Remediation Timeline
Critical	Within 72 hours
High	Within 14 days
Medium	Within 30 days
Low	Based on operational scheduling

Exceptions shall be documented and approved by management where immediate remediation is not operationally feasible.

12. Logging and Monitoring

Security logs shall be maintained for:

- User activity;
- Administrative actions;
- System events;
- Financial transactions;
- Authentication attempts.

Logs shall:

- Be protected from tampering;
- Be retained for the required regulatory period;
- Be reviewed regularly.

Monitoring controls shall support incident detection, forensic investigation, and regulatory reporting obligations.



13. Incident Management

13.1 Incident Reporting

All personnel must report suspected or actual security incidents immediately.

13.2 Incident Response

The Company shall maintain procedures for:

- Detection;
- Containment;
- Investigation;
- Recovery;
- Notification where required.

Security incidents shall be documented, investigated, escalated according to severity, and subject to post-incident review and remediation tracking.

Relevant evidence and forensic records shall be preserved where necessary for legal, regulatory, or investigative purposes.

13.3 Regulatory Notification

Where required by law or licensing obligations, relevant incidents shall be reported to the Curaçao Gaming Authority and other applicable authorities.

14. Business Continuity and Disaster Recovery

The Company shall maintain:

- Business continuity plans;
- Disaster recovery procedures;
- Backup systems;
- Recovery testing procedures.

Backups shall:

- Be encrypted;
- Be tested regularly;
- Be stored securely.

Disaster recovery and backup restoration procedures shall be tested periodically, at minimum annually.



Critical systems and services shall be prioritized according to operational and regulatory requirements.

15. Vendor and Third-Party Security

Third-party providers with access to Company systems or data shall:

- Undergo security due diligence;
- Sign confidentiality agreements;
- Maintain appropriate security controls;
- Notify the Company of security incidents affecting services.

The Company shall assess third-party risks periodically and maintain oversight of outsourced or cloud-hosted services relevant to regulated gaming operations.

16. Employee Awareness and Training

All employees shall receive periodic training covering:

- Information security awareness;
- Phishing and social engineering risks;
- Data protection obligations;
- Incident reporting procedures;
- Responsible system usage.

Training records shall be maintained.

Additional role-based security training may be provided for personnel with elevated access or security responsibilities.

17. Physical Security

Physical access to offices, servers, and infrastructure shall be restricted to authorized personnel.

Security measures may include:

- Access cards;
- CCTV monitoring;
- Visitor logs;
- Locked server rooms.



Physical security controls shall be appropriate to the sensitivity and criticality of the protected systems and information.

18. Compliance and Auditing

The Company shall periodically:

- Review this Policy;
- Conduct security assessments;
- Perform vulnerability testing;
- Conduct internal audits;
- Cooperate with regulatory audits.

Non-compliance may result in disciplinary action.

Security documentation and audit evidence shall be maintained in accordance with regulatory and operational requirements.

19. Policy Violations

Violations of this Policy may result in:

- Disciplinary action;
- Suspension of access rights;
- Termination of employment or contract;
- Regulatory reporting where applicable.



20. Policy Review

This Policy shall be reviewed:

- At least annually;
- Following major security incidents;
- Following significant operational or regulatory changes.



Appendix A – Incident Severity Classification

Severity	Description	Response Time
Critical	Major outage or data breach	Immediate
High	Significant operational impact	Within 1 hour
Medium	Limited impact	Within 1 business day
Low	Minor issue	As scheduled



Appendix B – Document Control

Version	Date	Description	Author
1.0	13.05.2026.	Initial version	Miroslav Munitlak