

Information Security Policy

Version 1.0.

1. PURPOSE AND OBJECTIVES

The purpose of this Information Security Policy (“Policy”) is to define the principles and responsibilities that ensure the confidentiality, integrity, and availability of information assets processed by Pomadorro N.V. (hereinafter “Pomadorro” or the “Company”).

The Policy aims to:

- Protect the Company’s digital and physical information assets from unauthorized access, disclosure, alteration, loss, or destruction;
- Safeguard Player Data and transactional information;
- Maintain compliance with applicable data protection, gaming, and financial regulations;
- Support business continuity and the resilience of iGaming systems and services;
- Ensure the secure flow of information, both within the Company and with external parties;
- Promote a culture of information security awareness among all personnel and partners.

The Policy aims to safeguard the Company, Company staff, its clients, partners and owners of intellectual property rights from information security related incidents, potential financial or reputational losses, operational impact, and any consequential action, loss of income or damage. The Policy also aims to establish control requirements on network systems, based on the International Standards ISO/IEC 27001 and ISO/IEC 27002.

2. SCOPE

This Policy applies to:

- All Company employees, contractors, consultants, suppliers, and third-party service providers;
- All information systems, platforms, and applications used by the Company;
- All data—personal, financial, operational, or otherwise—processed or stored by the Company;
- All end users (“Players”) whose personal and transactional data are handled by the Company in the course of gaming operations.

It covers:

1. Core gaming platforms, player account management (PAM) systems, payment and KYC modules;
2. Corporate systems and support tools;
3. Cloud services and hosted infrastructure.

3. INFORMATION SECURITY PRINCIPLES

The Company adheres to the following principles:

Confidentiality – Information shall be accessible only to authorized individuals with a legitimate business need.

Integrity – Information shall be accurate, complete, and protected against unauthorized modification.

Availability – Information and systems shall be available to authorized users when required to support operational continuity.

Accountability – All users are responsible for their actions in relation to Company systems and data.

Compliance – Information handling shall comply with applicable data protection laws, applicable gaming regulations, AML/CFT requirements, and internal company policies.

Risk-based approach – Security measures shall be proportionate to identified risks and regularly reviewed.

4. RESPONSIBILITIES

It is the responsibility of all users of the Company's information assets, systems, and networks to comply fully with this Policy. All users must act in a manner that safeguards the confidentiality, integrity, and availability of Company and, especially, Player Data.

The Company shall ensure that:

- This Policy is made available to all new employees, contractors, and partners upon engagement;
- Regular awareness and refresher training is provided to reinforce security practices;
- Any material updates to this Policy are communicated to all personnel and respective contractors (of needed) in a timely manner.

The Company recognizes that effective information management and protection are essential to:

- Maintain operational efficiency and resilience;
- Ensure legal and regulatory compliance (including applicable data protection laws and gaming regulations);
- Protect business continuity and corporate reputation;
- Support sound corporate governance and responsible data stewardship.

All employees, affiliates, contractors, suppliers, and partners who access or process Company information share the following responsibilities:

- To comply with this Policy and all related internal procedures and legal requirements;
- To access only the information necessary for their legitimate business function;
- To protect Company systems, accounts, and devices from unauthorized use;
- To refrain from knowingly violating or circumventing any information security control or allowing others to do so;
- Ensure that no individual should be able to access information to which they do not have a legitimate access right.

To immediately report any security incident, data breach, or suspicious activity using legal@pomadorro.com

The Company ensures that all Player Data is processed and stored securely in accordance with this Policy and applicable data protection legislation, and that appropriate technical

and organizational measures are implemented to prevent unauthorized access, alteration, misuse, or loss of information.

5. UNDERTAKINGS

The following roles and teams have defined responsibilities for ensuring the effective implementation and maintenance of information security across the Company's iGaming operations, infrastructure, and player services.

- a. **Management Board** is responsible for strategic oversight of information security and governance: (i) approves information security policies and resource allocation; (ii) ensures that information security objectives align with the Company's business strategy, compliance obligations, and regulatory framework; (iii) provides leadership in fostering a company-wide culture of data protection and responsible gaming integrity.
- b. **Cyber Security Team** is responsible for securing the Company's technical infrastructure, production environments, and networks supporting operations. This includes:
 - Managing infrastructure and application security in alignment with ISO/IEC 27001 standards;
 - Conducting vulnerability assessments and penetration tests;
 - Overseeing implementation of firewalls, encryption, and endpoint protection;
 - Providing expert guidance on information security risks and incident response;
 - Managing real-time monitoring, alerting, and remediation of potential threats;
 - Raising user awareness on phishing, credential security, and social engineering risks.
- c. **Data Protection Officer** is responsible for data protection and records retention issues.
- d. **Department Heads and Line Managers** are responsible for implementing and enforcing this Policy within their respective departments. They must ensure that:
 - Employees under their supervision follow Company security procedures;
 - Sensitive information (contracts, player communications, staff data, financial reports) is handled in accordance with classification rules;
 - Staff receive relevant awareness training and understand their data protection obligations;
 - Security incidents are promptly reported to the respective responsible team.
- e. **Project managers** are responsible for the information security of all data produced, shared, or processed during the lifecycle of development or operational projects. Their responsibilities include:
 - Ensuring that project deliverables incorporate security-by-design principles;
 - Managing secure communication and data exchange between internal and external stakeholders;
 - Ensuring risk assessments and access controls are applied to all project-related information;
 - Guaranteeing secure archiving, retention, and destruction of project documentation upon completion.
- f. **Business Led Technology Teams** are responsible for maintaining and securing the Company's operational systems and applications, including core gaming platforms, payment gateways, player account management (PAM) systems, KYC/AML modules, and business support tools (e.g. HR, Finance, CRM). Their duties include:

- Ensuring that all operational and player data is securely stored and processed;
- Identifying, assessing, and mitigating information security risks;
- Enforcing appropriate access controls and ensuring data is only accessible to authorized personnel;
- Maintaining backup, retention, disaster recovery, and secure data disposal procedures;
- Ensuring that any integrations with third-party systems (e.g. game providers, payment service providers, analytics tools) meet Company security requirements.

6. LEGAL & REGULATORY OBLIGATIONS

The Company stores and processes Player Data in secure data centres located in various jurisdictions where Pomadorro N.V. or its authorized service providers operate. This may involve transferring your personal data outside the European Union (“EU”) or the European Economic Area (“EEA”).

Some of these countries may not have been granted an adequacy decision by the European Commission. In such cases, the Company ensures that all international transfers are carried out in full compliance with applicable data protection laws. Appropriate safeguards are implemented to maintain the same level of protection as within the EEA — including the use of Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or other legally recognized transfer mechanisms.

The Company also complies with all gaming and gambling regulatory data obligations, including but not limited to player identity verification (KYC), anti-money laundering (AML/CFT), and responsible gambling requirements.

Details of these specific countries can be found here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

You may contact us at any time to obtain further details or request a list of our verified third-party service providers and data processing locations outside the EEA.

7. INFORMATION CLASSIFICATION

The table below outlines the information classification levels adopted by the Company, forming the foundation of its information security and data protection framework.

The classification level of information may be adjusted over time, depending on changes to its sensitivity, purpose, or regulatory requirements.

Security Level	Definition/ Access Control	Examples
Confidential	Accessible only to specifically authorized personnel within the Company who require such access to perform regulated or critical operational tasks. Must always be encrypted in transit and at rest, including on backup or third-party systems.	Personal Data that used by the Company for KYC/D under requirements of AML policy. • Player identity documents; • Player account login credentials; • Responsible gambling records and exclusion data; • Employee HR files; • System security keys, internal passwords.

Restricted	Accessible only to relevant departments, affiliates, or trusted partners under confidentiality obligations. Sharing or disclosure is limited to operational necessity.	• Player contact details (email, phone); • Account activity logs; • Business agreements, contracts, and NDAs; • Provider and PSP onboarding documentation; • Internal financial reports; • Customer support correspondence.
Public	Information approved for release into the public domain. No restriction on access or distribution, but content must be reviewed and authorized prior to publication.	• Website content and game descriptions • Marketing materials and press releases • Publicly available company policies (e.g. Responsible Gaming, Privacy Policy, Terms & Conditions) • Social media content officially managed by the Company

8. SUPPLIERS, PARTNERS, AND AFFILIATES

All third-party providers, affiliates, and business partners engaged by the company shall comply with this information security policy and maintain security standards equivalent to those required by the company.

This obligation applies to all external parties that:

- access, store, or process company data, player information, or system resources;
- integrate with or provide technology used for payment processing, game delivery, or marketing;
- operate remotely or on site within company systems; or
- subcontract services involving company or player data to other entities.

All such parties must sign appropriate data-processing and confidentiality agreements, undergo security due-diligence checks, and cooperate fully in case of an information-security investigation or audit.

9. COMPLIANCE, AWARENESS, AND DISCIPLINARY PROCEDURES

Compliance with this policy and all supporting information-security procedures is mandatory for every employee, contractor, or partner handling company or player data.

All new staff shall receive mandatory information-security and responsible-data-handling training as part of their onboarding. Refresher training shall be provided regularly or upon significant policy updates.

Employees and authorized users shall be informed of this policy and any amendments to it through official internal communication channels.

10. INCIDENT REPORTING AND RESPONSE

Any staff member, affiliate, or service provider who becomes aware of a potential or actual information-security or data-protection incident (including unauthorized access, data loss, or misuse) must immediately report it to **legal@pomadorro.com**.

All incidents shall be logged, investigated, and remediated promptly, with reports retained in accordance with regulatory and audit requirements.

Where required by law or regulation, affected players and relevant authorities shall be notified in accordance with applicable data protection legislation and local gaming regulations.

11. POLICY REVIEW AND CONTINUOUS IMPROVEMENT

This policy shall be reviewed regularly or if triggered by significant regulatory, technological, or organizational changes.

The review shall assess the effectiveness of current controls, identify new risks, and incorporate lessons learned from security incidents or audits.

Additional supporting procedures or sub-policies may be created or updated to address specific areas of information security.

All revisions shall be approved by the management board and communicated to staff and partners.