

PittaPlus Information Security Policy

1. Purpose and Scope This policy outlines the information security measures for PittaPlus. It applies to all employees, contractors, third-party service providers, and systems involved in the development, deployment, and management of our B2B gaming platform and corporate data.

2. Responsibility and Governance The Chief Technology Officer (CTO) is responsible for the overall implementation and daily management of information security. Executive management is responsible for reviewing and approving this policy.

3. Risk Management Information security risks are assessed at least annually by the CTO. Identified risks are recorded in a risk register, along with planned remediation actions to mitigate vulnerabilities.

4. Risk Themes Considered PittaPlus actively monitors and mitigates threats such as unauthorized system access, cyberattacks (e.g., ransomware, phishing), data leakage of corporate partner information, and critical service outages.

5. Access Control Access to PittaPlus systems and source code is strictly role-based and limited to business needs. Multi-Factor Authentication (MFA) is required for all critical systems. Access rights are immediately revoked when an employee or contractor leaves the company.

6. Data Protection and Privacy As a strictly B2B provider, PittaPlus does not collect or store B2C retail player data. We protect our corporate, financial, and partner data using standard encryption protocols. Data is retained only as long as legally or commercially necessary before being securely archived or deleted.

7. System and Network Security We utilize industry-standard technical safeguards, including firewalls, anti-malware software, and endpoint protection. Systems are regularly updated and patched to protect against known vulnerabilities.

8. Software Development and Change Management All updates or changes to the PittaPlus gaming software are tested in a secure staging environment. Changes must be reviewed and approved by the Lead Developer or IT Manager to ensure security standards are met before being deployed to the live production environment.

9. Incident Response In the event of a security breach, system outage, or data loss, the CTO must be notified immediately to contain the issue. As per CGA regulations, PittaPlus will officially report any critical incidents via the CGA portal within 24 hours.

10. Business Continuity and Disaster Recovery We utilize real-time automated database replication with weekly full system backups. All backups are stored securely on AWS. Restoration procedures are tested periodically to ensure rapid recovery of B2B operations in case of a disruption.

11. Third-Party and Vendor Security We evaluate the security posture of third-party vendors (such as AWS and other platform providers) before onboarding. We ensure that necessary security and confidentiality obligations are included in our vendor contracts.

12. Employee Awareness and Training All PittaPlus employees and relevant contractors must undergo basic information security training during onboarding. This includes awareness regarding phishing, password management, and acceptable use of company devices.

13. Monitoring and Logging System access, administrative actions, and network traffic are actively logged. These logs are reviewed by the IT team to detect suspicious activity and are retained securely to prevent unauthorized alteration.

14. Policy Review and Updates This Information Security Policy is reviewed annually by the CTO and executive management. It will also be updated following any major system changes, security incidents, or new regulatory directives from the CGA.

15. Contact Information For any questions or incident reporting regarding this policy, please contact the technology and security team at: **tech@pittaplus.com**