At SkillOnNet, information security is a fundamental component of our governance framework and critical to maintaining the trust of our players, partners, and stakeholders. As a gaming company handling sensitive player data and financial transactions, the organization is committed to protecting the confidentiality, integrity, and availability of all information assets.

An Information Security Management System (ISMS) is established, implemented, and maintained to support business objectives through a risk-based approach. Risk management is embedded within the organizational culture, including the identification, assessment, and mitigation of risks, supported by a maintained and regularly reviewed risk register. Controls are aligned with ISO/IEC 27001 to ensure a consistent and effective security framework.

Key information security commitments include:

- Protection of personal and sensitive data through strong access controls, secure system architecture, encryption, and continuous monitoring.
- Integration of security across operations, including secure development lifecycle practices, system hardening, and proactive threat detection and prevention capabilities.
- Secure processing of deposits, withdrawals, and financial transactions using encryption, fraud detection mechanisms, and adherence to financial security standards.
- Maintenance of the integrity of gaming software, databases, and backend infrastructure through regular security assessments and effective patch management.
- Compliance with applicable legal, regulatory, and contractual requirements, including data protection obligations, Anti-Money Laundering (AML) regulations, and gaming authority licensing requirements.
- Assurance of operational resilience through Business Continuity Plans (BCP) and Disaster Recovery (DR) strategies to maintain service availability and protect player data.
- Clear definition of roles and responsibilities for information security, supported by leadership commitment, adequate resourcing, and adherence by employees and third parties.
- Promotion of a strong culture of security awareness, accountability, and continuous vigilance across the organization.
- Implementation of effective incident management processes to detect, respond to, and recover from information security events.
- Ongoing monitoring, review, and continual improvement of the ISMS to address evolving threats, technological changes, and business needs

Management of SkillOnNet fully supports this policy and is committed to its implementation and continual effectiveness.