Erklärung zur Informationssicherheit

Bei SkillOnNet ist Informationssicherheit ein grundlegender Bestandteil unseres Governance-Rahmenwerks und entscheidend für die Aufrechterhaltung des Vertrauens unserer Spieler, Partner und Stakeholder. Als Spieleunternehmen, das mit sensiblen Spieldaten und finanziellen Transaktionen umgeht, verpflichtet sich die Organisation, die Vertraulichkeit, Integrität und Verfügbarkeit aller Informationswerte zu schützen.

Ein Informationssicherheitsmanagementsystem (ISMS) wird eingerichtet, implementiert und aufrechterhalten, um die Geschäftsziele durch einen risikobasierten Ansatz zu unterstützen. Risikomanagement ist in der Unternehmenskultur verankert, einschließlich der Identifizierung, Bewertung und Minderung von Risiken, unterstützt durch ein gepflegtes und regelmäßig überprüftes Risikoregister. Die Kontrollen sind an ISO/IEC 27001 ausgerichtet, um einen konsistenten und effektiven Sicherheitsrahmen zu gewährleisten.

Wichtige Verpflichtungen zur Informationssicherheit umfassen:
• Schutz personenbezogener und sensibler Daten durch starke Zugriffskontrollen, sichere Systemarchitektur, Verschlüsselung und kontinuierliche Überwachung.
• Integration von Sicherheit in alle Betriebsabläufe, einschließlich sicherer Entwicklungspraxis, Systemhärtung und proaktiver Bedrohungserkennung und -verhütung.
• Sichere Verarbeitung von Einzahlungen, Auszahlungen und finanziellen Transaktionen unter Verwendung von Verschlüsselung, Betrugserkennung und Einhaltung finanzieller Sicherheitsstandards.
• Wahrung der Integrität von Spielesoftware, Datenbanken und Backend-Infrastruktur durch regelmäßige Sicherheitsbewertungen und effektives Patch-Management.
• Einhaltung geltender gesetzlicher, regulatorischer und vertraglicher Anforderungen, einschließlich Datenschutzverpflichtungen, Anti-Geldwäsche (AML)-Vorschriften und Anforderungen an die Lizenzierung durch Spielbehörden.
• Sicherung der operativen Resilienz durch Business Continuity Plans (BCP) und Disaster Recovery (DR)-Strategien, um die Serviceverfügbarkeit aufrechtzuerhalten und die Spieldaten zu schützen.
• Eindeutige Definition von Rollen und Verantwortlichkeiten für die Informationssicherheit, unterstützt durch das Engagement der Führungsebene, angemessene Ressourcen und die Einhaltung durch Mitarbeiter und Dritte.
• Förderung einer starken Sicherheitskultur, Verantwortungsbewusstsein und kontinuierliche Wachsamkeit im gesamten Unternehmen.
• Implementierung effektiver Vorfallmanagementprozesse zur Erkennung, Reaktion und Wiederherstellung nach Informationssicherheitsereignissen.
• Laufende Überwachung, Überprüfung und kontinuierliche Verbesserung des ISMS, um sich entwickelnden Bedrohungen, technologischen Veränderungen und den Geschäftsanforderungen Rechnung zu tragen.

Das Management von SkillOnNet unterstützt diese Richtlinie vollumfänglich und verpflichtet sich zu deren Umsetzung und fortlaufender Wirksamkeit.