Declaración de Seguridad de la Información

En SkillOnNet, la seguridad de la información es un componente fundamental de nuestro marco de gobernanza y es fundamental para mantener la confianza de nuestros jugadores, socios y partes interesadas. Como empresa de juegos que maneja datos sensibles de jugadores y transacciones financieras, la organización se compromete a proteger la confidencialidad, integridad y disponibilidad de todos los activos de información.

Se establece, implementa y mantiene un Sistema de Gestión de Seguridad de la Información (SGSI) para apoyar los objetivos comerciales a través de un enfoque basado en riesgos. La gestión de riesgos está integrada en la cultura organizacional, incluida la identificación, evaluación y mitigación de riesgos, respaldada por un registro de riesgos mantenido y revisado regularmente. Los controles están alineados con la ISO/IEC 27001 para garantizar un marco de seguridad coherente y eficaz.

Los principales compromisos de seguridad de la información incluyen:
• Protección de datos personales y sensibles a través de controles de acceso sólidos, arquitectura de sistema segura, cifrado y monitoreo continuo.
• Integración de la seguridad en las operaciones, incluidas las prácticas del ciclo de vida de desarrollo seguro, el endurecimiento del sistema y la detección y prevención proactiva de amenazas.
• Procesamiento seguro de depósitos, retiros y transacciones financieras mediante cifrado, mecanismos de detección de fraudes y cumplimiento de estándares de seguridad financiera.
• Mantenimiento de la integridad del software de juegos, bases de datos e infraestructura de backend a través de evaluaciones de seguridad regulares y una gestión de parches eficaz.
• Cumplimiento de los requisitos legales, reglamentarios y contractuales aplicables, incluidas las obligaciones de protección de datos, las regulaciones de prevención de blanqueo de capitales (AML) y los requisitos de licencias de las autoridades de juego.
• Aseguramiento de la resiliencia operativa a través de los Planes de Continuidad de Negocios (BCP) y las estrategias de Recuperación ante Desastres (DR) para mantener la disponibilidad del servicio y proteger los datos de los jugadores.
• Definición clara de roles y responsabilidades para la seguridad de la información, respaldada por el compromiso del liderazgo, la dotación de recursos adecuada y la adherencia de empleados y terceros.
• Promoción de una cultura sólida de concienciación sobre seguridad, responsabilidad y vigilancia continua en toda la organización.
• Implementación de procesos de gestión de incidentes eficaces para detectar, responder y recuperarse de los eventos de seguridad de la información.
• Monitoreo, revisión y mejora continua del SGSI para abordar las amenazas en evolución, los cambios tecnológicos y las necesidades empresariales.

La dirección de SkillOnNet apoya plenamente esta política y se compromete a su implementación y eficacia continua.